NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements
September 2009 - Comment Resolution

Comment Number: 001	Submitted by: ODNI, DIA DSI-1, Angela Weis	Comment Type: _X_ Tech. __ Editorial __ Gen.
Reference: Section 2.3	Comment	
	Management and Accountability. Nothing in this section relates to holding people accountable for NOT following policies and practices.	
	Rationale/Recommendation	
	While audits are very important to verify policies and practices are being followed there is nothing about audit reporting; i.e., audits can be done but if the results are not reported and people held accountable for audit failures then this is meaningless.	
	Disposition	
	Audits and other enforcement activities are out of scope for the SGIP-CSWG. They are the responsibility of FERC and the state PUC's. Audit report is one of the requirements included in the NIST.	

Comment Number: 002	Submitted by: ODNI, DIA DSI-1, Angela Weis	Comment Type: _X_ Technical __ Editorial __ Gen.
Reference: Section 2.6	Comment	
	Use and Retention. There needs to be an explicit clause to address if in the course of collecting and analyzing data a crime is discovered that the information may be turned over to the appropriate law enforcement agencies.	
	Rationale/Recommendation	
	In a risk/reward, cost benefit analysis if it is cheaper to simply pay a fine then implement the needed changes then many companies may do just that, pay the fine rather than take steps/measures to get in compliance.	
	Disposition	
	Audits and other enforcement activities are out of scope for the SGIP-CSWG. They are the responsibility of FERC and the state PUC's. Also note that the issue of treatment of forensic evidence versus system restoration is explicitly identified in the Bottom Up discussion. There are requirements included in the NISTIR that address this concern.	

Comment Number: 003	Submitted by: ODNI, DIA DSI-1, Angela Weis	Comment Type: _X_ Technical __ Editorial __ General

<table>
<tr><td colspan="2">Comment Number: 003</td><td>Submitted by: ODNI, DIA DSI-1, Angela Weis</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Section 3</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Some of the categories list power outage as integrity impacts when it may be more appropriate to classify them as availability impacts.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Even if these categories were organized from a data centric view of the data flowing/processed by the specific categories, if bad data could cause outages then it would/should be true that if data isn't available then power outages could also occur.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">Power outage categorization has been changed in the updated version and now is classified under “power system reliability”. Impacts are now associated with Impact Categories.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 004</td><td>Submitted by: Kevin Sullivan
Senior Security Strategist
Trustworthy Computing
Microsoft Corporation</td><td>Comment Type: __ Technical __ Editorial X_ General</td></tr>
<tr><td rowspan="6">Reference:
Overall</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Due to the heavy reliance upon information and communications technology in the Smart Grid, there is a need for a new approach to risk management that enables a risk-based approach to security controls for the Smart Grid.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Create a risk management framework that is focused on protecting the functions of the electric power system rather than the individual assets and also accounts for the distributed nature of the Smart Grid.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">Several risk management frameworks are referenced within the document. A high-level Impact assessment has been developed within the document with respect to interface categories that can be cross referenced with applications specified in Chapter 2; specifically AMI, DGM, ES, ET, HAN/BAN and WASA.</td></tr>
</table>

Comment Number: 005	Submitted by: Kevin Sullivan Senior Security Strategist Trustworthy Computing Microsoft Corporation	Comment Type: _X Technical __ Editorial __General
Reference: None	Comment	
	Previous attempts to bolt security on late in the lifecycle (after development and deployment) have not worked in the past in other sectors and will not work in the Smart Grid. As technology is designed and developed for the Smart Grid is it important that vendors and integrators learn from the body of knowledge available such as secure software engineering practices including developer training, organizational processes, and tools.	
	Rationale/Recommendation	
	Identify secure development practices to improve the security of the thousands of software, hardware, and services components that will comprise the Smart Grid.	
	Disposition	
	Table 3.4 – Proposed Requirements for the Smart Grid identifies requirements found in the “DHS Catalog of Control Systems Security: Recommendations for Standards Developers” that address secure software engineering practices including training, organizational process, etc.	

Comment Number: 006	Submitted by: Kevin Sullivan Senior Security Strategist Trustworthy Computing Microsoft Corporation	Comment Type: _X_ Technical __ Editorial __General
Reference: None	Comment	
	The Smart Grid represents a shift from the relatively anonymous system we have today to one where strong authentication will provide benefits for both security and business purposes. This identity system will enable secure access to utility components as well as new customer scenarios for interacting with devices and service providers.	
	Rationale/Recommendation	
	Leverage and integrate cryptographically strong and robust (such as claims-based) identity management mechanisms into Smart Grid architectures. Such an “Identity Metasystem” will enable the trust decisions between millions of energy users, devices, systems and services while preserving customer privacy.	
	Disposition	
	We recognize the importance of strong authentication. This will be addressed in the next version of the NISTIR.	

Comment Number: 007	Submitted by: Kevin Sullivan Senior Security Strategist Trustworthy Computing Microsoft Corporation	Comment Type: _X Technical __ Editorial __ General
Reference: None	Comment	
	System owners and vendors must plan for rapid coordinated incident response spanning corporate and national boundaries and evolving over minutes and hours rather than weeks and months.	
	Rationale/Recommendation	
	Include the development of plans and processes for operational response into the Smart Grid security strategy. Sadly, Smart Grid components will have vulnerabilities and attackers will attempt to exploit them. Planning at this stage should focus on vulnerability and incident indications and warning mechanisms, incident response, threat containment, and vulnerability mitigation.	
	Disposition	
	In version 2, Incident response and incident response training are identified in Table 3.4 Proposed Requirements for the Smart Grid "DHS Catalog of Control Systems Security: Recommendations for Standards Developers" requirements 2.12.10 and 2.12.11. Table 5.1 "Standards Overview" also references the "Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Planning".	

Comment Number: 008	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: __ Technical __ Editorial _X_ General
Reference: 1.4.1	Comment	
	In this section of the Report, the selection of Use Cases is discussed. The Use Cases themselves are set out in Appendix A. APPA comments on Appendix A below; 3 suffice it to say here that the Use Cases need to take sufficient account of the privacy of customer information, and to accommodate a variety of business models.	
	Rationale/Recommendation	
	APPA appreciates the hard work and analysis that NIST put into the drafting of the Report. APPA files these comments to assist the drafters as they revise the Report, to ensure that the resulting work product will work for all segments of the industry as cyber security standards are implemented. APPA has been concerned throughout the NIST standards development process to date that the standards and protocols developed work —on the ground for all segments of the electric utility industry, including consumer-owned	

<table>
<tr><td colspan="2">Comment Number: 008</td><td>Submitted by: APPA, Susan N. Kelly
Vice President of Policy Analysis and General Counsel</td><td>Comment Type: __ Technical __ Editorial _X_ General</td></tr>
<tr><td></td><td colspan="3">public power systems, many of which are smaller electric utilities. It is easy for the concerns of these industry segments to get lost in the shuffle, since they often do not have the human and technical resources to devote to NIST‘s standard-drafting processes. However, consumer-owned utilities (public power systems and rural electric cooperatives) together serve 27 percent of the nation‘s electric consumers. NIST therefore needs to build sufficient flexibility into its cyber security requirements to accommodate the sizes and business models of consumer-owned systems.</td></tr>
<tr><td></td><td colspan="3">Disposition</td></tr>
<tr><td></td><td colspan="3">The Use Cases presented in appendix (A) are neither exhaustive nor complete. New Use Cases may be added as they evolve in future versions of this document. The use cases were derived “as-is” from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns. The section introduction has been modified to reflect this more clearly. NIST is making every effort to develop high-level security requirements that accommodate the various Smart Grid use cases.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 009</td><td>Submitted by: APPA, Susan N. Kelly
Vice President of Policy Analysis and General Counsel</td><td>Comment Type: __ Technical __ Editorial _X_ General</td></tr>
<tr><td>Reference: 2.2</td><td colspan="3">Comment</td></tr>
<tr><td></td><td colspan="3">APPA agrees with NIST that the lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed. Report at 8. Given the very substantial stimulus funds the Department of Energy has recently awarded for various Smart Grid proposals, it will be necessary in the very near future to address the privacy of customer information generated by Smart Grid installations. In doing so, regulators and the industry will have to weigh carefully the optimal combination of security measures and the consequences for a breach of privacy information.</td></tr>
<tr><td></td><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td></td><td colspan="3">APPA notes that some state regulators and their staff see the privacy of customer information as a, if not the, top priority issue associated with Smart Grid installations. At the recently concluded Winter Meeting of the National Association of Regulatory Utility Commissioners (NARUC), held on November 15–18, 2009, in Chicago, the NARUC Committee on Critical Infrastructure voted out Resolution No. CI-1, entitled Resolution Regarding Cybersecurity and Privacy Issues Surrounding Smart Grid. This resolution expressed strong concerns about the possibility that private customer data could be shared, misused, stolen or otherwise not adequately protected during Smart Grid program</td></tr>
</table>

Comment Number: 009	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: __ Technical __ Editorial _X_ General

deployments. In particular, it expressed concerns that third-party access to consumer data, particularly access to real-time usage information, could pose a physical threat to the consumer as third parties could monitor behavior patterns, such as whether a resident is home. The resolution called for the highest levels of consumer protections and cyber security. It further called upon NARUC to recommend federal legislation on cybersecurity and privacy issues be enacted as soon as possible that would put enforcement mechanisms in place that would ensure that any misuse or improper disclosure of consumer data, either intentional or through negligence, would be a federal crime with appropriate sanctions attached.

This resolution was tabled by NARUC‘s Board of Directors, due to concerns expressed about it by certain other NARUC Committees. APPA expects, however, that some form of resolution on these issues will again be considered at the next NARUC meeting, to be held on February 14–17, 2010, in Washington, D.C.

Proposals of this type (especially the possibility of federal criminal liability for even negligent disclosures of customer information) are of substantial concern to APPA. NIST and those drafting cyber security standards under its auspices need to be fully aware of the strong concerns of these state regulators surrounding the privacy of customer information. In response, NIST needs to do two things. First, it needs to ensure that its cyber security standards incorporate into Smart Grid architecture all reasonable, cost-effective safeguards to protect the privacy of customer information. Second, it needs to educate state and federal policy makers as to the potential costs and benefits of including the —highest level of cyber security safeguards into Smart Grid installations.

As Ms. Annabelle Lee of NIST noted in her telephonic presentation on Tuesday, November 17, 2009, at the NARUC Concurrent Session on The Cyber House Rules: What Regulators Need to Know about Cybersecurity, disclosures of customer data, while certainly unwanted, will be almost inevitable, as meters will be compromised, and it is virtually impossible to provide 100 percent protection 100 percent of the time from data disclosures. Emphasis on mitigation of such disclosures is therefore appropriate. Further, it could be prohibitively expensive to include the —highest level of cyber security safeguards into Smart Grid installations, especially for smaller electric utilities. NIST itself appropriately acknowledges this cost-benefit trade-off in Appendix A at A-3, when it states [b]alance is also needed between risk and the cost of implementing the security measures. The combination of very expensive required safeguards and severe punitive measures for even negligent breaches of customer information could be enough to induce many smaller utilities to take a “thanks, but no thanks” attitude to Smart Grid installations. NIST therefore needs to balance all of these factors in developing its cyber security safeguards, and to educate policy makers about the wisdom of the choices that it makes.

Disposition

We have developed a cyber security strategy and performed a high level risk assessment to develop recommended security requirements to be used as a starting point for organizations as input into their cyber security

Comment Number: 009	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: __ Technical __ Editorial _X_ General

	strategy and risk assessment. The privacy chapter has been revised and includes new privacy practices.

Comment Number: 010	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X Technical __ Editorial __ General

Reference: 2.5.3	Comment
	These sections of the Report discuss personally identifiable information (PII). APPA generally finds the principles for PII set out in Section 2.3 to be reasonable, but notes that if carried out to the fullest extent, some could handicap electric utilities in carrying out their core reliability functions. Even today, electric utilities provide customer-specific information to third parties in carrying out their utility functions. For example, if there is a customer outage, electric utilities might share that outage information, including specific customer information, with third-party contractors or crews from other electric utilities assisting in the restoration of service. If utilities were required to obtain customer-by-customer consent to such disclosures, their efforts to restore service could be delayed. Since one of the purposes of Smart Grid installations is to pinpoint more accurately customer outages, it seems like overkill to require individual customer sign-off on such information disclosures. On the other hand, APPA certainly understands that PII collected from a customer should not be disclosed without his or her prior permission to vendors or other entities for purposes removed from the utility‘s core functions—for example, commercial marketing purposes. APPA‘s point is that disclosure requirements should not be so onerous as to interfere with utility service to electric customers.
	Rationale/Recommendation
	None.
	Disposition
	NIST agrees that organizations should have disclosure requirements and it is up to each organization to develop specific disclosure requirements. These disclosure requirements need to meet applicable laws and regulations. The privacy chapter has been revised and includes new privacy practices.

Comment Number: 011	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X Technical __ Editorial __ General

Comment Number: 011	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X Technical __ Editorial __ General
Reference: 2.5.10	Comment	
	This section states that —[p]rivacy protections should be applied consistently and at the same level for all PII throughout the entire Smart Grid system to be effective. Report at 14. APPA is concerned that this concept, if applied literally, could require a small consumer-owned utility to implement all of the same privacy protections for PII that the largest of investor-owned utilities would employ, regardless of the cost of the necessary systems and the personnel to maintain such safeguards. A —rule of reason will have to be applied, or the perverse result would be that consumers served by smaller utilities will not have access to Smart Grid technology. While all utilities should implement appropriate safeguards for PII, those safeguards do not necessarily have to be at the same level to be effective.	
	Rationale/Recommendation	
	None.	
	Disposition	
	We acknowledge this comment and have revised the document to remove the referenced text.	

Comment Number: 012	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	This section of the report gives an initial set of AMI security requirements. APPA assumes these requirements will be developed further and the final list may become standards that utilities may need to comply with. Therefore, APPA recommends that the requirements be clear, non-prescriptive, cost effective and scalable based on the criticality of the device or system. The following comments are to assist the drafting team in creating achievable requirements. APPA commends the Cyber Security Coordination Task Group (CSCTG) (now SGIP-CSWG) for including suggestions for best practices on policy, procedures, document management, continuity of operations and compliance. However, the focus of these requirements should be on Smart Grid cyber security.	
	Rationale/Recommendation	
	The following requirements from Chapter 4 are better suited for a guidance document in support of these requirements; APPA therefore requests that they be excluded from the final requirement section:	
	Disposition	

Comment Number: 012	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X Technical __ Editorial __ General

	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 013	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4	Comment
	DHS-2.16.14/ NIST SP 800-53 CA-1 Security Policy Compliance APPA believes that a utility must create a culture of cyber security awareness within the organization and the best way to accomplish that is through strong internal policies and procedures. Having a clear division between requirements for Smart Grid system functionality and the process to secure those systems would help utilities understand the requirements. The following is a non-exhaustive list of those requirements that APPA feels may be key policies and procedures for inclusion in a System Security Management requirement, similar to the North American Electric Reliability Corporation (NERC) CIP-007 Standard:
	Rationale/Recommendation
	None
	Disposition
	We are working very closely with NERC as the new versions of the CIP requirements are drafted. The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 014	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General

<table>
<tr><td colspan="2">Comment Number: 014</td><td>Submitted by: APPA, Susan N. Kelly
Vice President of Policy Analysis
and General Counsel</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference: Chapter 4</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">DHS-2.15.29/ NIST SP 800-53 SC-7 Use of External Information Control Systems

APPA recommends careful wording of these requirements so that they cover the cyber functionality, but are not so prescriptive as to limit a utility‘s ability to provide innovative, cost-effective solutions to cyber security challenges. APPA also cautions NIST on using existing standards as minimums for these requirements. For example, DHS-2.8.12.2, Supplemental Guidance, states as follows: Any cryptographic modules deployed within an AMI system, at a minimum, must be able to meet the Federal Information Processing Standard (FIPS) 140-2. Report at 63 (emphasis added). Another example is DHS-2.15.14/ NIST SP 800-53 IA-7 Cryptographic Module Authentication: Must comply with FIPS 140-2[.] Report at 102.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Although APPA feels that the FIPS model is a thorough and useful process for the federal government with its need to cover all hazards, APPA is concerned that it is not a cost-effective standard for the NIST Smart Grid Cyber Security requirements process. The NIST requirements should only recognize the FIPS model as one option available for a utility to use for compliance with these requirements, and should allow for other methods of compliance, especially for smaller utility systems.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">Cryptography and key management are critical security issues for the Smart Grid and will be addressed more completely in the next version.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 015</td><td>Submitted by: APPA, Susan N. Kelly
Vice President of Policy Analysis
and General Counsel</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="2">Reference: Chapter 4</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">APPA also advises NIST to avoid statements of opinion and confusing language in these requirements; for example: The use of collaborative computing mechanisms on AMI components is strongly discouraged[.] Report at 63. If this is a standard, it cannot be strongly discouraged. Similarly, DHS-2.8.8.2, Supplemental Guidance, states: When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization must either implement appropriate compensating security measures or explicitly accepts the additional risk. Report at 61.</td></tr>
</table>

Comment Number: 015	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
	Rationale/Recommendation	
	APPA agrees that the use of appropriate compensating security measures should be an option, especially in the case of legacy systems. APPA is confused, however, by the reference to acceptance of additional risk. Does this mean that the standard could be met merely by acceptance of the additional risk? Further clarification of this point is required.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 016	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	APPA is concerned that DHS-2.8.7.1 Requirement incorporates unclear statements that may be taken as opinion. That standard states: In AMI, the very concept of boundaries is problematic. Internal systems within the organization may be more easily protected than components which reside outside significant physical boundaries and controls. Meters and poll-top and other systems without significant controls and external monitoring cannot be amply secured and should always be considered relatively untrusted. Report at 60. This statement assumes that the utility could not mitigate this risk through upgrades in technology, changing of operating procedures or by other means yet to be devised.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

<table>
<tr><td colspan="2">Comment Number: 017</td><td>Submitted by: APPA, Susan N. Kelly
Vice President of Policy Analysis and General Counsel</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Chapter 4</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">The text of DHS-2.8.7.2 Supplemental Guidance acknowledges it is evaluating only the current state in cyber security for this technology: At this time components and systems connected to the Internet constitute a substantial increase in risk for the core functionality of the AMI system. (Emphasis added.) This admits that at some future time the use of the internet may be a secure communication path, which therefore should not be categorically excluded from use. Also, some of the text is contradictory. For example, in DHS-2.8.7.2, guidance item #1 it states: Generally, no AMI system information should be publicly accessible. However, guidance item #2 states: The organization must prevent public access into the organization‘s internal AMI system networks except as appropriately mediated and monitored.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">This guidance should not be included unless it is made clear what the organization must do to secure communication paths in order to be in compliance.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 018</td><td>Submitted by: APPA, Susan N. Kelly
Vice President of Policy Analysis and General Counsel</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="4">Reference:
Chapter 4</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">APPA advises the drafting team to avoid requirements that dictate how to comply with a standard or requirement. Unduly prescriptive requirements curb each utility‘s ability to come up with innovative, least-cost options. For example, DHS-2.8.18.2 Supplemental Guidance states: The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information must be documented, tracked, and audited periodically. After identifying these connection points, the extent of their protection needs to be determined. Report at 65.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">APPA recommends that if the drafting team wants to give a list of suggested solutions or guidance, these items</td></tr>
</table>

Comment Number: 018	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
	should be included in a guideline that supports the requirement, rather than being made part of the requirement.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 019	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix A	Comment	
	In Appendix A (at A-2), NIST sets out three key security requirements (Integrity, Availability, and Confidentiality) for the Use Cases that follow. NIST then states that [c]onfidentiality is generally the least critical [security requirement] for actual power system operations, although this is changing for some parts of the power system, as customer information is more easily available in cyber form. As APPA has noted above, for certain state regulators, confidentiality is of the utmost importance, to the point that they favor federal legislation that would make even negligent breaches of customer information a federal crime.	
	Rationale/Recommendation	
	APPA therefore again urges NIST to follow a two-track approach regarding this issue: (1) ensuring that its cyber security standards incorporate into Smart Grid architecture all reasonable and cost-effective safeguards to protect the privacy of customer information, while also (2) educating state and federal policy makers as to the potential costs and benefits of including the highest level of cyber security safeguards into Smart Grid installations.	
	Disposition	
	We are focusing on reliability since it is first priority to the power grid but we do realize that confidentiality is important. We definitely want to coordinate with state and federal policy makers in developing this NISTIR.	

Comment Number: 020	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General

Reference: Use Cases	Comment
	Turning to the actual Use Cases, APPA notes with appreciation that certain of the use cases/scenarios, e.g., Real Time Pricing (RTP) for Customer Load and DER/PEV (at A-10-11) and Time of Use (TOU) Pricing (at A-11-12), specifically state that demand response can be implemented in many different ways, and that rate designs can differ from utility, being either real-time or tariff-based. It is important that the use cases build in such flexibility, so that different rate designs and business models can be fully accommodated. On the other hand, the Bulk Power Electricity Market use case/scenario still appears to assume one form of wholesale power supply market—the centralized markets run by Regional Transmission Organizations (RTOs). This case‘s Category Description states (at A-20) that [t]he market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. The Scenario Description states that the bulk power market varies from region to region and is conducted primarily through Regional Transmission Operators (RTO) and Independent System Operators (ISO). Id. NIST should be aware that state regulators and legislators in many regions of the country have decided not to implement retail electric industry restructuring or to proceed with RTOs/ISOs at the wholesale level, including the Southeast, Desert Southwest, Mountain West and Pacific Northwest. APPA does not anticipate Order No. 2000-compliant RTOs forming in these regions any time soon.
	Rationale/Recommendation
	This scenario should therefore be revised to reflect the continuing regional diversity in wholesale power markets.
	Disposition
	The Use Cases presented in appendix (A) are neither exhaustive nor complete. New Use Cases may be added as they evolve in future versions of this document. The use cases were derived “as-is” from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns. The section introduction has been modified to reflect this more clearly.

Comment Number: 021	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General

Reference: Retail Power Electricity	Comment
	The Retail Power Electricity Market scenario/use case needs to be revised. While the Category Description notes that the electricity market varies significantly from state to state, region to region and at local levels, it goes on to state

Comment Number: 021	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
Market scenario/use case	that [t]he market is still evolving after some initial setbacks, and is expected to expand from bulk power to retail power and eventually to individual customer power as tariffs are developed to provide incentives. This description fails to take into account current regulatory realities. Many states did move to implement retail restructuring of their electric utilities in the late 1990s, but after the debacle in California, and the failure of retail restructuring over time to fulfill the promise of lower electric rates in many states, states that had not done so largely decided to stay put. This situation shows little signs of changing, although vertically integrated utilities in these regions have shown increasing interest in Smart Grid installations and time-differentiated rate designs.	
	Rationale/Recommendation	
	Revise Retail Power Electricity Market scenario/use case.	
	Disposition	
	The Use Cases presented in appendix (A) are neither exhaustive nor complete. New Use Cases may be added as they evolve in future versions of this document. The use cases were derived “as-is” from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns. The section introduction has been modified to reflect this more clearly.	

Comment Number: 022	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix A	Comment	
	Consumer-owned electric utilities generally did not implement retail restructuring, even if they were located in regions where investor-owned utilities were restructured. These utilities are owned by their consumers and continue to be vertically integrated. Consumer-owned utilities generally see their role as helping their customers manage energy usage, price volatility and overall bills, rather than simply stepping back and letting their retail customers experience the full brunt of volatile wholesale market pricing (whether they want it or not). As noted above, consumer-owned utilities currently serve 27 percent of the United States’ electric consumers.	
	Rationale/Recommendation	
	For all of these reasons, the Retail Power Electricity Market use case/scenario needs to be revised to accommodate the full range of retail electric utility business models, rather than assuming an unjustified evolutionary path.	

Comment Number: 022	Submitted by: APPA, Susan N. Kelly Vice President of Policy Analysis and General Counsel	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	The Use Cases presented in appendix (A) are neither exhaustive nor complete. New Use Cases may be added as they evolve in future versions of this document. The use cases were derived “as-is” from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns. The section introduction has been modified to reflect this more clearly.	

Comment Number: 023	Submitted by: EEI, James P. Fama	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	It is important for NIST to recognize that each electric utility has very specific and potentially unique implementation and deployment requirements. While it is clear that Smart Grid products of the future must have security “built-in” as part of design, one-size-fits-all solutions are not appropriate. For example, future products may not address an electric utility’s particular operational requirements and its legacy equipment. NIST should provide additional discussion in the Draft NISTIR explaining how each potential subject entity should carefully evaluate their performance and security objectives and choose appropriate security mechanisms based upon fact-specific risk analysis and prioritization.	
	Rationale/Recommendation	
	EEI encourages NIST to collaborate closely with the electric utility industry to develop options for integrating legacy equipment into a smarter grid.	
	Disposition	
	Several representatives from the utility industry participate in the SGIP-CSWG, and we welcome anyone who wants to participate. We have revised the document to clarify that the content is at a high level – and each organization will need to address security based on their specific systems.	

Comment Number: 024	Submitted by: EEI, James P. Fama	Comment Type: __ Technical __ Editorial _X_ General
Reference:	Comment	

Comment Number: 024	Submitted by: EEI, James P. Fama	Comment Type: __ Technical __ Editorial _X_ General

1.1 & 1.3	See the Draft NISTIR at 1. It is also helpful that NIST is publishing this preliminary report that describes the CSCTG's (now SGIP-CSWG) overall security strategy for the Smart Grid, as well as distilling use cases collected to date, requirements and vulnerability classes identified in other relevant cyber security assessments and scoping documents, and other information necessary for specifying and tailoring security to provide adequate protection for the Smart Grid. Alternatively, it is not clear whether the Draft NISTIR is intended to be a template for regulatory requirements, which EEI believes would be inappropriate. EEI urges NIST to revise the Draft NISTIR to clearly state that implementers of the Smart Grid Framework and Roadmap (e.g., utilities, equipment manufacturers and regulators) should use it as a tool in developing an appropriate Smart Grid Cyber Security strategy in conjunction with Smart Grid development.
	Rationale/Recommendation
	EEI appreciates that NIST has established a Smart Grid Cyber Security Coordination Task Group ("CSCTG") (now SGIP-CSWG) and agrees that cyber security is critical to all of the particular priority application plans discussed in the NIST Smart Grid Framework 1.0 document. However, EEI suggests that sections 1.1 and 1.3 of the Draft NISTIR should be clarified with respect to the purpose and intent of this document. For example, it is not clear whether this document is to be used as a guide/reference with examples that can be used in the development of security plans for individual and unique Smart Grid development.
	Disposition
	We have added additional text to clarify that this is guidance and not mandatory.

Comment Number: 025	Submitted by: EEI, James P. Fama	Comment Type: __ Technical __ Editorial _X_ General

Reference: Overall	Comment
	EEI suggests that the Draft NISTIR should be revised to make clear that it is limited to serving as strategy guide for developing Smart Grid security requirements and should be clear that it does not serve as an "auditable check-list." The Draft NISTIR should provide a clear strategy and a "tool kit" that provides both guidance and methods to resolve conflicts between operability and security requirements for all stakeholders. Hence, one example of such a necessary revision to the Draft NISTIR is that it should be titled as "Smart Grid Cyber Security Strategy." This is an appropriate title for the NISTIR because it reflects that currently no equipment manufactured meets all the "Requirements" that are described in the Draft NISTIR.
	Rationale/Recommendation

Comment Number: 025	Submitted by: EEI, James P. Fama	Comment Type: __ Technical __ Editorial _X_ General

	The Draft NISTIR should be revised to make clear that it does not create Smart Grid Cyber Security “requirements,” but rather is a strategy document intended to facilitate the development of such requirements through the SGIP/SGIPGB processes.
	Disposition
	The content of the document is a set of recommended cyber security requirements. The text has been revised to clarify that this is guidance, and is not mandatory.

Comment Number: 026	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Appendix A	Comment
	Since the Use Cases in Appendix A are not comprehensive, this appendix should be revised to make clear that the Use Case are not mandatory. Furthermore, the Use Cases in Appendix A of the Draft NISTIR should be revised to eliminate statements that imply broad and general requirements. The following are some non-exhaustive examples of such statements that should be either eliminated or qualified:
	Rationale/Recommendation
	None
	Disposition
	The Use Cases presented in appendix (A) are neither exhaustive nor complete. New Use Cases may be added as they evolve in future versions of this document. The use cases were derived “as-is” from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns. The section introduction has been modified to reflect this more clearly.

Comment Number: 027	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4	Comment
	The Draft NISTIR proposes that “AMI components should only push traffic to the home area network.” See Draft NISTIR at 60 (citing to DHS-2.8.7.2 Supplemental Guidance). However, this appears to be in direct conflict with the direction coming from the Open SG Security team and EEI understands that at least one utility has attempted a one-

Comment Number: 027	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

	way-only-system that simply did not work. EEI therefore recommends the NISTIR adopt language similar to that used in Open SG's Security Profile for Advanced Metering Infrastructure(see DHS-2.8.7.4 Rationale, page 29 – 30) which states that: "the most secure option would allow for one way communications from the NAN to the HAN and not allow data to flow from the HAN to the NAN. The requirements identified in the OpenHAN SRS establish the need for two way communications between the NAN and HAN to meet the industry's long term functional goals. The addition of two way communications between the NAN and the HAN introduces additional risk for unauthorized access to the AMI system. Similarly, the utility NAN, wired or wireless, will offer attackers potential entry points into the network. For these reasons, compartmentalization of the AMI system and boundary protection should be employed to mitigate risk and limit the impact of unauthorized access to as small of portion of the AMI system as possible."
	Rationale/Recommendation
	None
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 028	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4	Comment
	The Draft NISTIR states that "[c]onnections to the Internet and other public networks is discouraged for AMI systems." See Draft NISTIR at 60 (citing to DHS-2.8.7.2 Supplemental Guidance). This broad statement appears to inappropriately severely limit the communication options for this interface.
	Rationale/Recommendation
	EEI understands that there are risks associated with using the Internet and public networks for AMI systems, but instead of broadly discouraging use of the Internet and public networks for AMI systems, the NISTR should describe the risks and the appropriate risk mitigation methods associated with the use of the Internet and "public networks" for AMI systems.

Comment Number: 028	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 029	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4

Comment

The Draft NISTIR includes the term “cryptographic mechanisms.” See Draft NISTIR at 61 (citing to DHS-2.8.8.3 Requirement Enhancements). However, this term is not be clearly defined since it does not set forth the minimally acceptable cryptographic mechanisms or whether it would be sufficient to simply "mask" the data, which is a form of a cryptographic mechanism. Furthermore, this term does not make clear whether AES128 or AES 256 is the minimum applicable standard.

Rationale/Recommendation

None

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 030	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Appendix A

Comment

The Draft NISTIR states that “[a]bsolute security may be achievable, but is undesirable because of the loss of functionality that would be necessary to achieve this near perfect state.”

Comment Number: 030	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

	Rationale/Recommendation
	This statement should be revised to state: “Although absolute security would be desirable, but because it is unachievable . . . .”
	Disposition
	The statement has been revised to read, “Absolute security is never perfectly achievable, so the costs and impacts on functionality of implementing security measures must be weighed against the possible impacts from security breaches.”

Comment Number: 031	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Overall	Comment
	None
	Rationale/Recommendation
	EEI recommends that the NISTIR should be revised to define the term “Cyber Security” as “measures taken to maintain the confidentiality, availability, and integrity of data, computer networks and systems.”
	Disposition
	We have revised the definition of cyber security to be more inclusive of the IT, Telecommunications, and electric sectors.

Comment Number: 032	Submitted by: EEI, James P. Fama	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 3	Comment
	None
	Rationale/Recommendation
	EEI suggests that Chapter 3 of the Draft NISTIR should be revised to be an additional appendix and should be titled: Potential Examples for a Logical Interfaces. This revision would be appropriate because each deployment will be unique in its system architecture and therefore a “one size fits all” approach would be impractical and burdensome.

<table>
<tr><td>Comment Number: 032</td><td>Submitted by: EEI, James P. Fama</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Furthermore, NIST should work with the industry to develop a “Risk Matrix” as a tool for decision-making with respect to operability and security requirements.</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">The emphasis is on logical architecture and the logical interface information to assist in the selection of security requirements. The document has been revised to clarify that it is guidance, not mandatory.</td></tr>
</table>

<table>
<tr><td>Comment Number: 033</td><td>Submitted by: EEI, James P. Fama</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference: Appendix B</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">With respect to Appendix B, EEI believes that it does not make clear which document should be followed for each security requirement in the Draft NISTIR. Appendix B is not sufficiently clear because in most cases, it appears that the Draft NISTR refers to more than three documents that could be relevant, but does not identify or provide a method of resolving any conflicts between these documents.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">EEI believes that utilities would find it helpful to have a tool to help resolve conflicts between relevant standards. Providing such explanation would also be valuable since not all entities have the resources to obtain licensed documents. EEI on behalf of its members companies, respectfully requests that NIST ensure that future actions in developing the Smart Grid Interoperability Standards Roadmap be consistent with the foregoing recommendations. Finally, EEI wishes to commend NIST for its efforts in developing the Draft NISTIR and to express appreciation to NIST for the opportunity to comment.</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">The security requirements included in the second draft of the NISTIR are from several documents listed in Appendix B. In addition, in the next version of the NISTIR other documents will be reviewed for appropriate security requirements. All of the referenced documents are source documents for the NISTIR. Currently, only the NERC CIPs are mandatory.</td></tr>
</table>

<table>
<tr><td>Comment Number: 034</td><td>Submitted by: NERC</td><td>Comment Type: __ Technical __ Editorial _X_ General</td></tr>
<tr><td>Reference:</td><td colspan="2">Comment</td></tr>
</table>

Comment Number: 034	Submitted by: NERC	Comment Type: __ Technical __ Editorial _X_ General
Overall	The Smart Grid Cyber Security Document describes NIST’s overall cyber security strategy for the Smart Grid by analyzing use cases, requirements and vulnerability classed identified in other cyber security assessments and scoping documents, and other information necessary for specifying and tailoring security requirements to provide adequate protection for the Smart Grid. NIST states that ultimately, the Smart Grid Cyber Security Coordination Task Force will develop a comprehensive set of cyber security requirements. The Smart Grid Cyber Security Document is the first step in the development of a set of cyber security requirements applicable to the Smart Grid. NERC’s comments herein focus on suggested areas for NIST’s further consideration in the development of a cyber security strategy for the Smart Grid, and how the overall cyber security strategy should influence the development of a set of cyber security requirements.	
	Rationale/Recommendation	
	As discussed below, there are very important cyber security considerations that will impact the Smart Grid that NERC believes must be included in NIST’s overall cyber security strategy. As a general matter, NIST discusses the importance of interfaces in the Smart Grid Cyber Security Document and explains how these interfaces will come together to create the Smart Grid. NERC agrees that these interfaces are important, and recommends that Interoperability and System Security Standards be developed that apply directly to the integrators and the equipment being integrated to ensure that requirements are in place to support interconnection one system to another. While the focus in the Smart Grid Cyber Security Document is on devices, developing a better communications gateway or smart meters will not ensure the integrated devices will provide sufficient cyber security of the Smart Grid. Issues will arise in the integration of these systems that will require attention. One method NERC recommends for NIST’s consideration in the development of an overall cyber security strategy of the Smart Grid is to develop standards that apply to the integration of these systems required for use by their integrators. NERC discusses these concepts in more detail below in its discussion of specific sections of the Smart Grid Cyber Security Document.	
	Disposition	
	We will be looking at design consideration in the next draft of the NISTIR.	

Comment Number: 035	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.2	Comment	
	In Section 1.2 of the Smart Grid Cyber Security Comments, NIST states that, in accordance with the Energy	

Comment Number: 035	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General

Independence and Security Act of 2007, the U.S. will support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth.[1] There are two objectives that NIST states will be important in achieving a Smart Grid. These are:

1. [The] [i]ncreased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid; and
2. Dynamic optimization of grid operations and resources, with full cyber-security ...[2]

While NERC agrees these two categories are important areas in achieving a Smart Grid, NERC notes that there is no such thing as full cybersecurity. That is, there is no "cyber security model" that, once achieved, will ensure full protection of the Smart Grid. There currently is no cyber security model that will accomplish complete security of the Smart Grid. Therefore, it is important that NIST understand that there are different levels of maturity involving the Smart Grid, and integration of new parts and pieces into the Smart Grid could present cyber risks because there is no industry-accepted cyber security strategy.

Rationale/Recommendation

NERC proposes two strategies in developing a cyber security framework for the Smart Grid:

1. In an organized and designed way, NIST and the industry need to develop a focus on response and recovery. While the first goal of a cyber security strategy should be on prevention, it also requires that a response and recovery strategy be developed in the event of a cyber attack on the electric system. More planning and investment is needed to develop response and recovery actions, while continuing to develop a strategy for prevention of a cyber security incident.
2. It is essential that those parts or equipment of the Smart Grid that optimize the system are separate from the core components of the Smart Grid. The core components are those components that are essential to enabling a functioning electric grid. Therefore, the core components of the Smart Grid must be understood so that, in the event of a cyber security incident the grid, the core components can be recovered with minimal technology in a quick and efficient manner, thereby assuring bulk power system reliability. This attention on the core components of the Smart Grid will also help identify where response plan decisions and actions can be carried out to protect core functionality and/or quickly restore it.

Disposition

The NISTIR is a high level document addressing response, recovery, and prevention. Each organization will need

[1] *Id.* at p. 2.
[2] *Id.*, citing to EISA of 2007, P.L. 110-140.

Comment Number: 035	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
	to define the core components of their respective Smart Grid deployments.	

Comment Number: 036	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.3	Comment	
	In Section 1.3 of the Smart Grid Cyber Security Document, NIST states that "[c]yber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters." NIST continues that "[v]ulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways." Given the seriousness of potential cyber security vulnerabilities on the Smart Grid, NERC believes it is critically important that NIST's assessment of an overall cyber security strategy for the Smart Grid be more inclusive than what is presented in the Smart Grid Cyber Security Document because it will affect the operation of the electric system from generation to meter.	
	Rationale/Recommendation	
	One suggestion NIST should consider is to expand its risk assessment to address three components: distribution, transmission and generation. The Smart Grid will equally create risk across all three of these functions. Additionally, there will be an increased potential for attacks, not only in those areas where electrons flow for power, but also where communications take place. With the Smart Grid, significant technology additions will be made in the distribution environment, thereby introducing the possibility of cyber security attacks on the distribution system. Section 1.3: NIST's Discussion Regarding Overall Risk to the Electric System Should be More Inclusive Because the Smart Grid Will Affect the Electric System from Generation to Meter.	
	Disposition	
	The first version of the NISTIR focused more on the AMI sector. The second draft of the NISTIR expands to look at the entire Smart Grid.	

Comment Number: 037	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.3	Comment	
	In Section 1.3 of the Smart Grid Cyber Security Document, NIST states that, "[w]ith the adoption and implementation of the Smart Grid, the IT and telecommunications sectors will be more directly involved," and it	

Comment Number: 037	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
	therefore proposes that IT and telecommunications cyber vulnerabilities for these areas be assessed in the context of Smart Grid.	
	Rationale/Recommendation	
	While NERC agrees that the introduction of new IT and telecommunications equipment will introduce tools to the Smart Grid that are more mature than some current industrial control applications, having the ability to protect these new applications (i.e. IT and telecommunications) from cyber security risk will not guarantee that the Smart Grid as a whole is protected from a potential cyber attack.	
	Disposition	
	The first version of the NISTIR focused more on the AMI sector. The second draft of the NISTIR expands to look at the entire Smart Grid.	

Comment Number: 038	Submitted by: NERC	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	NERC and NIST must carefully assess any potential cyber security impacts on the Smart Grid and the work that is required to ensure that potential cyber security risk is effectively managed in light of newly discovered cyber security vulnerabilities. Many Smart Grid users are just now considering the Supervisory Control and Data Acquisition (“SCADA”) environment. Therefore, even if cyber security practices are working in the IT and telecommunications realm, a system more impervious to cyber attacks requires additional work in an integrated, embedded, system control and network environment. The bulk power system is made up of large amounts of system inertia, and existing control systems are used to manage a very large, nonlinear system. Cyber security strategy that works for one area (e.g. IT or telecommunications) cannot be assumed to effectively be applied in a Smart Grid environment where new tools and equipment will be integrated to make up the Smart Grid, thereby potentially introducing new cyber security vulnerabilities on a regular basis.	
	Rationale/Recommendation	
	None	
	Disposition	
	The first version of the NISTIR focused more on the AMI sector. The second draft of the NISTIR expands to look at the entire Smart Grid. As we continue work on the document, we will continue our analysis to ensure that we include all security requirements for distribution, transmission, generation, and customer use.	

Comment Number: 039	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.3	Comment	
	NIST concludes Section 1.3 by defining cyber security as the “protection required to ensure confidentiality, integrity and availability of the electronic information communication system.”[3] While this definition focuses on the information communications system in cyber security of the Smart Grid, it is not a broad enough definition to ensure adequate cyber security of the Smart Grid. Rather, it leaves the impression that the lack of cyber security or the impact of cyber security vulnerabilities are confined only to the information communication systems of the Smart Grid. This is not the case. Potential cyber security vulnerabilities could apply to all areas of the Smart Grid, including the performance of physical equipment. That is, cyber security implications can materially impact the industry’s ability to provide commands that actually transpose the boundary from a cyber command communication to a Remote Terminal Unit (“RTU”) specifying an operating voltage to a device that results in a physical action (i.e. the opening or closing of a switch).	
	Rationale/Recommendation	
	NIST’s definition for cyber security must include more than just those elements that are linked to the information and communication systems.	
	Disposition	
	We have revised the definition of cyber security to be more inclusive of the IT, Telecommunications, and electric sectors.	

Comment Number: 040	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall Section 1.4.2	Comment	
	In Section 1.4.2, NIST explains its risk assessment of the Smart Grid by identifying potential vulnerabilities and describing how it examined the impacts and threats to the Smart Grid from both a high-level overall functional perspective as well as a focus on the six functional priority areas that are the focus of the Smart Grid cyber security strategy. NIST explains that the output will be used in the selection of security requirements and identification of security requirement gaps. Based on its risk assessment, NIST proposes an overall cyber security strategy for the Smart Grid, including proposed cyber security standards that should be included in the body of Interoperability Standards.	

[3] *Id.* at p. 3.

Comment Number: 040	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General

NIST's overall risk assessment is flawed because it does not capture the essential idea that Smart Grid is not a point in time. That is, one specific action cannot be taken regarding cyber security that will protect the system as a whole. Because the Smart Grid will evolve in pieces and parts, every time a new piece or part is integrated into the Smart Grid, new system vulnerabilities and variations on consequences could be introduced. Very rarely will the introduction of a new piece or part take vulnerabilities away. Therefore, when they are integrated into the Smart Grid, that piece or part must be customized to ensure that cyber security is integrated into system architectures. Additionally, there must be a continuous focus on cyber security protection of equipment that is integrated into the Smart Grid from a bulk power system planning design and operation perspective. Anytime a new piece or part is introduced, an assessment of potential cyber security vulnerabilities and consequences if successfully exploited is required so the industry can adequately protect that equipment from a potential harm. This process must be well-defined, continuous with the growth of the Smart Grid, and coordinated amongst the industry.

Rationale/Recommendation

One approach that NIST should consider in ensuring that the process of continually assessing cyber security risks to the Smart Grid is performed is to develop a common lexicon or language to capture system or function vulnerabilities that require continual monitoring of cyber security weaknesses. This common lexicon could be modeled after the Mitre Common Weakness Enumeration ("CWE") or a similar, common enumeration. The CWE provides a common language of discourse for discussing, finding, and dealing with the causes of software security as they are found in code, design, or system architecture. A similar lexicon could be developed to enable the discussion of cyber security vulnerabilities, particularly for those potential cyber security vulnerabilities and risks of the Smart Grid. This common lexicon will also help to enable the secure planning, design and operation of the bulk power system.

For example, today NERC might receive a message from a Reliability Coordinator regarding its SCADA system indicating that it "lost visibility." However, because there are no agreed-upon definitions, industry stakeholders may not necessarily know the context or ramification for this statement. Therefore, the development of a common lexicon will support the industry in understanding what is meant by providing a clearer understanding of what actions are needed to protect the security of the electric grid.

Additionally, because the Smart Grid will be developed in components, pieces, or systems, each one should have its own method of communicating to the system its operational status. With these methods of communication, each system's operational status could be communicated in such a way that a system operator will immediately know whether a system is vulnerable to cyber security attacks and therefore, what the vulnerabilities are and if the components, pieces or systems should be interconnected. A system's operational status could be categorized in three categories: (1) a "fully capable" system is a system that is capable of doing all of the things that is needs to do and is believed to be cyber-secure; (2) a "degraded" system is a system that can only do certain things without cyber risk; and (3) a "not capable" system is a system that is not capable of performing its primary mission, and as such, requires that

Comment Number: 040	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General

it be taken out of operation.

These three categories describing operational status of systems are one method of providing the industry with the tools it needs to understand what the problems are with respect to cyber security risk for the systems that will make up the Smart Grid. These considerations should be considered in the planning side too. Ultimately, a common lexicon to assess cyber security risk, along with a method of assessing a system's operational status, will provide a better view to the industry of potential cyber security vulnerabilities and what losses to a system mean for the reliability and security of the electric grid.

Disposition

Currently, reporting vulnerabilities for controls systems falls under the responsibility of DHS and DOE. We will consider this recommendation in a future draft of the NISTIR.

Comment Number: 041	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General

Reference: Overall Section 1.4.4

Comment

In Section 1.4.4 of the Smart Grid Cyber Security Document, NIST states that currently only NERC CIP Reliability Standards are mandatory for a specific domain of the Smart Grid. In fact, NERC's Reliability Standards not only apply to a specific domain of the Smart Grid, they also only apply to specific parties. While NERC agrees that cyber security is a top priority, NERC CIP Reliability Standards are not intended to reach beyond the reliability of the bulk power system. Therefore, caution should be used in applying NERC CIP Reliability Standards to an overall cyber security strategy for the Smart Grid to ensure cyber security protection of Smart Grid devices.

The applicability of NERC-developed, FERC-approved CIP Reliability Standards is limited to users, owners and operators of the bulk power system in accordance with Section 215 of the FPA. However, Smart Grid technologies and applications will generally be applied at the customer and distribution system levels, which are not typically considered to be part of the bulk power system. Therefore, the aggregated impacts of these Smart Grid devices on the bulk power system could be substantial.

While the purpose of developing Interoperability Standards is to ensure that Smart Grid systems can freely exchange information without logical barriers, the NERC CIP Reliability Standards purposefully put barriers in place to protect the various elements that comprise the critical infrastructure assets of the bulk power system, including critical cyber assets, from malicious intrusion or attack. As such, NIST must recognize that its application of the NERC CIP Reliability Standards to the overall cyber security strategy for the Smart Grid will not, by themselves, adequately protect cyber security of all components of the Smart Grid, such as Smart Grid distribution devices.

Additionally, NERC's CIP Reliability Standards do not provide requirements for actual components, such as the

Comment Number: 041	Submitted by: NERC	Comment Type: _X_ Technical __ Editorial __ General

requirement for device-to-device authentication. While the CIP Reliability Standards are designed to shape the behavior of asset owners and operators, they are not designed to shape the behavior of equipment and system designers, manufacturers and integrators. The CIP Reliability Standards apply to installed equipment and require security controls be applied to manage risk in the operation and maintenance of cyber assets. However, the protection goals of the Smart Grid, on the other hand, are broader, and address component security, integrity of communications, privacy and other cyber security considerations.

Rationale/Recommendation

Accordingly, NIST should integrate adequate cyber security protection, at all levels (device, application, network and system) in the development of a cyber security strategy for the Smart Grid that goes beyond the requirements of NERC CIP Reliability Standards. While NERC CIP Reliability Standards provide for the reliable and safe operation of the bulk power system by preventing the unauthorized cyber and physical access to critical assets and critical cyber assets, there is a need to develop a broader approach to prevent cyber security vulnerabilities on the Smart Grid in the overall cyber security framework. NERC's CIP Reliability Standards focus on protecting the integrity of the bulk power system rather than on components or specific functions. While NERC's CIP Reliability Standards require identification of bulk power system components that are material to the reliability of the bulk power system, they do not focus on the ability to serve customers on all elements of the bulk power system or on the protection of those elements. Therefore, NIST's cyber security strategy for the Smart Grid should integrate cyber security protection for those parts of the Smart Grid that the CIP Reliability Standards cannot protect.

NERC believes the cyber security strategy for the Smart Grid should focus on potential cyber security vulnerabilities of Smart Grid technologies and their associated network and system architectures, with an eye toward pass-through attacks (i.e. an attacker moving from a point in the system to other critical infrastructure systems) and aggregated impacts to the bulk power system. NERC intends to work closely with NIST through the Cyber Security Coordination Task Group and the Smart Grid Interoperability Panel in the development of an overall cyber security strategy for the Smart Grid.

Section 1.4.4: NIST States that the NERC CIP Standards are Mandatory for a Specific Domain of the Smart Grid. This is not accurate. NERC's Reliability Standards Only Apply to Users, Owners, and Operators of the Bulk Power System.

Disposition

The NISTIR has been modified to reflect this recommendation. We are looking at the entire Smart Grid and acknowledge that the only mandatory standards at this time are the NERC CIPs.

<table>
<tr><td colspan="2">Comment Number: 042</td><td>Submitted by: NERC</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="4">Reference: overall</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">In Chapter 3, NIST analyzes the interface diagrams for the six functional priority areas provided in the Smart Grid Framework Document, and identifies the logical data flows within each interface diagram, identifying the security constraints and issues for each interface. The logical interfaces in the six functional priority areas were allocated to one of fifteen different categories, and within each of these fifteen categories, the confidentiality, integrity and availability impact levels of data compromises at each interface was examined. While NIST’s analysis is useful in examining some of the potential cyber security vulnerabilities of the Smart Grid, it does not adequately describe the impacts of a vulnerability on each interface in such a way that will allow the industry to adequately determine how to prioritize cyber security protection and recovery of the systems and parts that will make up the Smart Grid.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">One suggested approach that will provide the industry with the information it needs to prioritize cyber security protection and recovery of the core components of the Smart Grid is to include in Chapter 3 an examination of the core capabilities of the six functional areas explored. Because not all control systems are equal, and many system enhancements will enable grid optimization only, it is essential that the industry have a mechanism in place in which the core capabilities can be defined and separated from those parts of the Smart Grid that optimize the grid. While NERC supports an optimized grid, NERC believes it is more important that the industry have the capability to segment the essential core components of the Smart Grid so that in the event of a high risk or incident, the core components can be addressed first and preserved to maintain bulk power system reliability. Accordingly, it will be essential to distinguish between core components and optimization functions.
For example, in Section 3.3, NIST examines the category of “[c]ontrol systems with high data accuracy and high availability, as well as media and compute constraints,” and provides as an example systems that are “[b]etween SCADA and field equipment.” NIST then goes on to examine the constraints and issues associated with this scenario. While an examination of the potential constraints and issues associated with this scenario is useful, NERC believes an additional category examining the core equipment should be included because only certain parts of “[c]ontrol systems with high data accuracy and high availability, as well as media and compute constraints” are core components. This additional analysis will provide the information that the industry needs to examine which equipment merely optimizes the Smart Grid, and which equipment is vital for a functioning electric grid. For example, the ability to keep SCADA systems running is a core requirement.
Once these core components are determined, an additional analysis of the “confidentiality,” “integrity,” and “availability” categories must be analyzed so that the industry understands which of these categories are core functions. Core functions will be those parts of the Smart Grid that must be preserved under a complete failure mode. Therefore, understanding what is core is essential to ensuring a grid safe from cyber security attacks.
For example, pages 22 and 23 of the Smart Grid Cyber Security Document describes the category “[b]ack office</td></tr>
</table>

<table>
<tr><td>Comment Number: 042</td><td>Submitted by: NERC</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="3"></td><td colspan="2">systems under common management authority," includes the subcategory "integrity," in which NIST states that the "[l]oss of integrity of data can cause power outages, including massive outages if meters are disconnected without authorization." NIST continues that the "[l]oss of integrity of data could cause safety hazards for utility personnel, customer, and property." NERC believes these considerations could be expanded to include an analysis of the core functions. That is, NIST could include in its analysis an examination of the disconnection or reconnection of meters without authorization, because, from a power balancing perspective, while the loss of power to thousands of homes is significant, the industry must also consider the impacts of the reconnection happening too fast. If the disconnection or reconnection happens too fast and in a large scale, it will be extremely difficult to balance that system. Therefore, NERC encourages NIST to expand its view of the scenarios provided in Chapter 3 to examine the core functions. By doing so, if there is a core component or function, it will be known to the industry at the time or even before a potential incident. This will provide the industry with the necessary tools to prioritize the safety and preservation of the core components and functions over equipment that is for optimization purposes only. An examination of core components and functions will also help the industry develop a plan to bring those core components back online as quickly as possible in the event of a cyber security vulnerability
While NERC believes the use cases provided in Chapter 3 are useful because they help the industry consider potential concerns associated with the Smart Grid, the impacts analyzed miss an important point that needs to be examined. The category definitions should be looked at with what would be the core components of that category in the event of a system operating in a "fully capable" mode, a "degraded" mode, or a "not capable" mode. Additionally, some of the use cases analyzed in Chapter 3, while important, should not command a higher priority with respect to cyber security protection and recovery if they are not core components that drive the electric system. Accordingly, the core components should be clearly examined and separated from those components that merely provide optimization of the Smart Grid.</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">Each organization will need to define the core components of their respective Smart Grid deployments. This information should be used in the development of the cyber security strategy and the selection of security requirements.</td></tr>
</table>

<table>
<tr><td>Comment Number: 043</td><td>Submitted by: ATIS</td><td>Comment Type: __ Technical __ Editorial _X General</td></tr>
<tr><td rowspan="2">Reference: Overall</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">The Alliance for Telecommunications Industry Solutions (ATIS) appreciates the opportunity to offer comments on the initial draft of the (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements (NIST Smart Grid Cyber</td></tr>
</table>

<table>
<tr><td>Comment Number: 043</td><td colspan="2">Submitted by: ATIS</td><td>Comment Type: __ Technical __ Editorial _X General</td></tr>
<tr><td rowspan="5"></td><td colspan="3">Security Requirements). Given the critical and interconnected role that the information technology and communications (ICT) sector plays in supporting the implementation of Smart Grid, ATIS strongly supports NIST's efforts to identify and assess the security vulnerabilities and design in security requirements at the design phase of the Smart Grid.
The purpose of these comments is to make NIST's Smart Grid Cyber Security Coordination Task Group (CSCTG) (now SGIP-CSWG) aware of ATIS' standards development efforts and other work related to cyber security in the ICT sector which may be helpful as the CSCTG refines this initial draft of its NIST Smart Grid Cyber Security Requirements.
ATIS is very interested in the Smart Grid implementation and recently submitted comments[1] to the NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft), in which ATIS is listed as one of the collaborating standards development organizations. Additionally, this past summer ATIS participated in NIST workshops aimed at developing the roadmap for Smart Grid standards.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">NIST recognizes that security must be built in from the beginning. NIST will expand on this in the next version.</td></tr>
</table>

<table>
<tr><td>Comment Number: 044</td><td colspan="2">Submitted by: ATIS</td><td>Comment Type: __ Technical __ Editorial _X_ General</td></tr>
<tr><td rowspan="4">Reference: Appendix D</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">While ATIS supports NIST's efforts to develop cyber security standards related to Smart Grid, ATIS is concerned that statements in Appendix D.4 Openness and Accessibility of Smart Grid Standards could be misconstrued to imply that simply because there is a charge for a standard that the standard is not "accessible." Neither openness nor accessibility demands that documents be made available without charge. Many standards development organizations, including ATIS, recover the costs of their activities through nominal document fees and such fees are essential to the development of standards. The terms "open" or "openness" describe the collaborative, balanced and consensus-based approval process used to develop standards. This process includes opportunity for broad-based public review and comment as well as opportunity for appeal if due process principles are not respected. ATIS follows such processes and promulgates open standards that are publically available and accessible.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">ATIS agrees that "secretly developed" algorithms or protocols may be a cause for concern. However, ATIS does not believe that standards developed through the open standards development process described above require either that the documents be made available for free or that the intellectual property (IP) owners must relinquish their rights.</td></tr>
</table>

Comment Number: 044	Submitted by: ATIS	Comment Type: __ Technical __ Editorial _X_ General
	Instead, ATIS believes that it is important to balance the interest of those who will implement such standards with the interest of the IP owners.	
	Disposition	
	The second sentence of section 3.1 of the Bottom Up document clearly agrees that IEEE, ANSI, IEC, etc. standards are open - just not as open as IETF standards. Nevertheless, the wording in the second paragraph was changed to avoid possible confusion in associating these standards with closed, secretly developed algorithms.	

Comment Number: 045	Submitted by: ATIS	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	According to this initial draft of the NIST Smart Grid Cyber Security Requirements, cyber security refers to “the protection required to ensure confidentiality, integrity, and availability of the electronic information communication system.” It is clear to see that the ICT sector will be integral to the implementation of the Smart Grid.	
	Rationale/Recommendation	
	Assessing telecommunications network circuit diversity should be a component of the overall cyber security evaluation of Smart Grid. To ensure that the telecommunications infrastructure that supports Smart Grid is resilient in the event of physical destruction of network facilities (central offices, outside plant, etc.), telecommunications circuits that provide key operations must be redundant and have diverse pathways. The ATIS National Diversity Assurance Initiative (NDAI) (report published in February 2006), provides a comprehensive overview of the process involved to determine if telecommunications circuits are truly diverse at the street level. The NDAI effort was conducted to evaluate diversity assurance for the Federal Reserve Bank. This assessment model can be readily applied to evaluate circuit diversity in other sectors, including energy.	
	Disposition	
	We have revised the definition of cyber security to be more inclusive of the information technology, telecommunications, and electric sectors. The emphasis of the NISTIR is on overall requirements for the Smart Grid and that diverse pathways and redundancy are potential controls to meet these requirements.	

Comment Number: 046	Submitted by: ATIS	Comment Type: __ Technical __ Editorial _X General
Reference: Appendix D	Comment	
	ATIS forums, including the Chief Information Officer (CIO) Council, the Optical Transport and Synchronization	

Comment Number: 046	Submitted by: ATIS	Comment Type: __ Technical __ Editorial _X General

Committee (OPTXS), and the IPTV Interoperability Forum (IIF), are engaged in developing work products related to cyber security.

ATIS' Chief Information Officer (CIO) Council, which provides a venue for CIO-level executives from among the largest service provider companies to identify and discuss information technology (IT) issues, is addressing the IT impacts related to cyber security. The ATIS CIO Council is currently examining the Cybersecurity Act of 2009 and has formed an Enterprise Risk Management (ERM) Working Group to explore three specific areas related to the cyber security legislation, including the potential impacts to carriers, technical implications, and providing public comments.

The cyber security aspects of Smart Grid will also be affected by the timing and synchronization performance. The ATIS Optical Transport and Synchronization Committee (OPTXS) develops standards that focus on telecommunication equipment that transport voice, data, and video over copper and fiber and its OPTXS-Synchronization (SYNC) Subcommittee concentrates on the synchronization aspects including accurate generation and distribution of timing (time/frequency) signals. OPTXS-SYNC may add value in the evaluation of security risks caused by modifications that violate Ethernet layering functions. In addition, OPTXS-SYNC would be able to assist in evaluating performance impacts caused by security countermeasures in relation to their suitability especially for packet-based timing applications.

ATIS notes that Appendices D.17 and D.24 of the NIST Smart Grid Cyber Security Requirements highlight the importance of developing key management standards to Smart Grid cyber security. ATIS' IPTV Interoperability Forum (IIF), which enables the interoperability, interconnection, and implementation of IPTV systems/services, has published several standards involving authentication protocols and security robustness relative to IPTV. These standards include: ATIS-0800024 Security Robustness Rules Interoperability Specification and ATIS-08000014 Secure Download and Messaging Interoperability Specification. Some of the concepts contained in these documents may be applicable to the ongoing work in NIST on Smart Grid.

Rationale/Recommendation

None

Disposition

Thank you for the references.

Comment Number: 047	Submitted by: GridWise Alliance-Katherine Hamilton	Comment Type: __ Technical __ Editorial _X General

Reference: Overall

Comment

Thank you for allowing the GridWise Alliance to provide comments as NIST and its stakeholders develop the NIST Interagency Report (NISTIR). Our group has been reviewing the NISTIR and has some overarching comments. The

Comment Number: 047	Submitted by: GridWise Alliance-Katherine Hamilton	Comment Type: __ Technical __ Editorial _X General
	GridWise Alliance believes it will be important to focus on the objectives and needs for standards and cyber security as facilities deploy Smart Grid technologies.	
	Rationale/Recommendation	
	We think vendors and asset owners alike will need guidance to ensure that a robust cyber security regime is in place. We also think the privacy issue should be handled separately and should be removed from this document. The NISTIR should focus instead on the specificity of standards pertaining to cyber security rather than data privacy.	
	Disposition	
	Both reliability and privacy are being addressed by the NISTIR.	

Comment Number: 048	Submitted by: Sensus- Sandy Bacik	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	Sensus would like to see NIST establish more clarity how this document will evolve to address emerging threats, Smart Grid paradigms and other changing elements of Security.	
	Rationale/Recommendation	
	None	
	Disposition	
	This document will be continually revised to address changes in technology and the threat environment.	

Comment Number: 049	Submitted by: Sensus- Sandy Bacik	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	The NISTIR 7628 document takes a mainly top-down approach to threat assessment, vulnerability categorization and some threat modeling. There is a CSCTG (now SGIP-CSWG) Bottom-up group, Sensus would like to suggest a threat assessment and modeling from the bottom-up and intermediate threat surfaces to develop a more robust view of current threats as well as emerging attacks such as workflow/process white space, return-oriented programming, SSL spoofing and other potential vectors.	
	Rationale/Recommendation	
	None	

Comment Number: 049	Submitted by: Sensus- Sandy Bacik	Comment Type: __ Technical __ Editorial _X General
	Disposition	
	These were considered in developing both the bottom-up and vulnerability classes chapters of the NISTIR.	

Comment Number: 050	Submitted by: Sensus- Sandy Bacik	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	There have been general conversations about the efficacy of "Smart Grid Security Certification" and the ability for government, regulatory and/or private entities to address this *potential* need. With NIST taking the lead on recommending the cyber security standards, Sensus would like to see NIST take the lead on taking a stand as to whether such certification is warranted, and if so start to establish some guidance in this area. Conversely, if NIST feels this is an unwarranted area for them to address, then clearly state that position. And what assistance from the UCAIug SG Conformity WG will be in the future document releases?	
	Rationale/Recommendation	
	None	
	Disposition	
	The SGIP Testing and Certification Committee has been established to focus on this issue. Any individual is encouraged to participate in the SGIP process. NIST SGIP-CSWG will be coordinating with this new committee.	

Comment Number: 051	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.4.4, page 6:	Comment	
	Sections within this document identify several wireless technologies, including 802.11, when discussing Cyber-Security Strategy areas to be addressed.	
	Rationale/Recommendation	
	The Wi-Fi Alliance recommends that the IEEE 802.11 standards (e.g. 802.11-2007, 802.11n, etc.) be included in the list of standards directly relevant to Smart Grid. As deployments of this technology already exist within the current Smart Grid, the CSCTG should review the security aspects of these standards when considering Smart Grid security requirements.	

Comment Number: 051	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	Currently PAP 2 under the SGIP is addressing this issue.	

Comment Number: 052	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: __ Technical _X_ Editorial __ General
Reference: Page 13 Clause 2.5.5	Comment	
	Existing Text: The new smart meters, and the Smart Grid network, will have the capability to use the collected data in an unlimited number of ways. Information should only be used or disclosed for the purpose for which it was collected, and should be divulged only to those parties authorized to receive it.	
	Rationale/Recommendation	
	Suggested Change: The new smart meters and the Smart Grid network will have the capability to use the collected data in an unlimited number of ways. However, authorization must be obtained before the information is used. Information shall only be used or disclosed for the purpose for which it was collected, and should be divulged only to those parties authorized to receive it. On reading, the impression is that lots can be done, but this will not be permitted. The intent is lots can be done, but authorization is needed first.	
	Disposition	
	Use and disclosure of energy usage data are addressed in the privacy practices included in Chapter 4 of the NISTIR.	

Comment Number: 053	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 18 Clause 3.3	Comment	
	Existing Text: Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls (either physical or cryptographic) appropriate for wireless.	
	Rationale/Recommendation	
	Suggested Change: Replace referenced text with --- Wireless media is often less expensive than wired media, and thus is attractive for many applications. It also provides additional deployment flexibility in many environments. Wireless deployments require cryptographic security controls appropriate for the wireless application. Physical security	

Comment Number: 053	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical __ Editorial __ General
	for wireless communications is not a viable option. Cryptographic solutions are required and should be mandated.	
	Disposition	
	We agree with this comment and have revised the reference section of the NISTIR.	

Comment Number: 054	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical _ Editorial __ General
Reference: Page 58 DHS-2.8.3.2	Comment	
	Existing Text: 5. Passwords and/or security keys should be of limited value, avoiding significant reuse of keys or passwords between different components and users. For example, compromising one key must not allow compromise of an entire network.	
	Rationale/Recommendation	
	Suggested Change: 5. The scope of passwords and/or security keys should be limited to the intent of their usage. Significant reuse of keys or passwords between different components and users should be avoided. The example appears to disable centralized management of any system.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 055	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 108 Clause DHS-2.15.26.3 part 2	Comment	
	Existing Text: The organization shall use authentication and cryptography or enhanced defense mechanisms to protect wireless access to the AMI system. Wireless technologies include, but are not limited to, microwave, satellite, packet radio [UHF/VHF], 802.11, 802.15, 802.16, cellular, ZigBee, ISA100, WiHART, and Bluetooth. 2. The organization shall scan for unauthorized wireless access points at a specified frequency and takes appropriate action if such access points are discovered. Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact AMI components. The scan is not limited to only those areas within the facility containing the high-impact AMI components.	

Comment Number: 055	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical __ Editorial __ General

	Rationale/Recommendation
	Suggested Change: Replace referenced part 2 with: 2. The organization shall scan for unauthorized wireless transmitters and base stations at a specified frequency and takes appropriate action if unauthorized devices are discovered. Organizations conduct a thorough scan for unauthorized wireless transmitters and base stations in facilities containing high-impact AMI components. The scan is not limited to only those areas within the facility containing the high-impact AMI components. The guidance describes possible technologies that include microwave, satellite, packet radio [UHF/VHF], 802.11, 802.15, 802.16, cellular, ZigBee. The further requirements are specific to scanning for unauthorized access points which is largely an 802.11 terminology. Serious threats of rogue devices exist for all wireless technologies and the wording should be inclusive. Access point scanning should be replaced by unauthorized transmitter scanning to include Bluetooth, Zigbee and all wireless technologies.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 056	Submitted by: WiFi Alliance- Greg Ennis	Comment Type: _X_ Technical _ Editorial __ General

Reference: Page D-5 Clause D-13	Comment
	Existing Text: Secure end-to-end communications protocols such as TLS ensure that confidentiality and integrity of communications is preserved regardless of intermediate hop.
	Rationale/Recommendation
	Suggested Change: Add reference to IPsec as follows -- Secure end-to-end communications protocols such as TLS and IPsec ensure that confidentiality and integrity of communications is preserved regardless of intermediate hop. IPsec will be more appropriate for some classes of devices.
	Disposition
	This comment has been addressed in the second draft of the NISTIR.

<table>
<tr><td>Comment Number: 057</td><td colspan="2">Submitted by: WiFi Alliance- Greg Ennis</td><td>Comment Type: _X_ Technical _ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Page D6
Clause D16</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Existing Text: “Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself”.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Suggested Change: Change "primarily because of the distributed nature of the system itself" to "because it is outside the scope of routing protocols".
Routing protocols provide an efficient path to get from A to B in a robust way that scales and deals with node failure. It is up to something else to define how to protect the data that is routed on the routes a routing protocol comes up with.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">This comment has been addressed in the second draft of the NISTIR.</td></tr>
</table>

<table>
<tr><td>Comment Number: 058</td><td colspan="2">Submitted by: WiFi Alliance- Greg Ennis</td><td>Comment Type: _X_ Technical _ Editorial __ General</td></tr>
<tr><td rowspan="4">Reference:
Page D-6
Clause D-16</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Existing Text: Modern mechanisms like 802.11i have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without routing security, attacks such as eavesdropping, impersonation, man-in-the-middle, and denial-of-service could be easily mounted on AMI traffic.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Suggested Change: Replace referenced text with: Modern mechanisms like 802.11i and 802.11w have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without end-to-end security (like IPsec), attacks such as eavesdropping, impersonation, man-in-the-middle, and could be easily mounted on AMI traffic. Routing security will be required to prevent denial-of-service attacks.
Like 802.11i, IEEE 802.11w is relevant in closing some of these holes. Also, multi-hop communications of any</td></tr>
</table>

Comment Number: 058 | Submitted by: WiFi Alliance- Greg Ennis | Comment Type: _X_ Technical _ Editorial __ General

type needs end-to-end security in addition to link security. Routing security is important for L2 and L3 and can be provided by end-to-end layering or by routing-specific techniques. If the data path is protected by an end-to-end mechanism, routing attacks are largely DoS.

Disposition

This comment has been addressed in the second draft of the NISTIR.

Comment Number: 059 | Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang | Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2

Comment

NIST's work to develop a Smart Grid cyber security strategy, including recommendations for protecting consumer privacy in the modernized grid, is a vitally important effort. The transition to the Smart Grid promises great benefits for consumers, including lowered energy costs, increased usage of environmentally-friendly power sources, and enhanced security against attack and outage. At the same time, it presents new risks to consumer privacy. At the core of the modernized grid's functionality is fine grained household data; in order to enable more efficient energy use and to more actively engage individual consumers and their appliances in energy management, the Smart Grid, as currently envisioned by proponents, depends on the collection and use of highly granular consumption data. Recent experiments using the simplest data mining and pattern matching techniques reveal how easily this information can be analyzed to expose intimate details about activities within the home with a high degree of accuracy.

Rationale/Recommendation

None

Disposition

NIST continues to update its recommendations regarding privacy and the Smart Grid (now included in chapter four).

Comment Number: 060 | Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang | Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2

Comment

From a consumer privacy perspective, we stand at a critical juncture in the development of Smart Grid technologies

Comment Number: 060	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

	for several reasons. First, the emergence of increasingly sophisticated metering technologies are enabling the unprecedented collection of energy consumption data, removing a “latent structural limitation” that previously protected the revelation of intimate details about household activities. Whereas historically a consumer’s consumption data may have been collected once a month or less frequently from a traditional meter fixed to the side of a house, in the Smart Grid, sophisticated new demand response systems will collect a record of 750 to 3,000 data points a month, revealing variations in consumption that can reflect specific household activities such as sleep, work, and travel habits. Second, the transition to a highly-interconnected and less-bordered electrical infrastructure is inviting participation by new entities, such as third-party service providers offering new web-based portals for managing energy use, who are utilizing consumer data in new ways and presenting the need for privacy analysis extending beyond the more straightforward consumer-to-utility relationship. Third, the rapid pace of Smart Grid deployment, and the speed at which new Smart Grid technologies are moving out of the pilot project stage to large-scale implementation, is making the consideration of the consumer privacy issues presented by these technologies more urgent. Finally, against this landscape of rapid development, there remains a “lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use,” creating “a privacy risk that needs to be addressed,” as prudently noted in the NIST Draft.
	Rationale/Recommendation
	None
	Disposition
	NIST continues to update its recommendations regarding privacy and the Smart Grid (now included in chapter four).

Comment Number: 061	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2	Comment
	Against this backdrop, NIST’s work to coordinate Smart Grid standards will ensure there is a common set of widely supported open protocols governing the modernized grid. But there is also an urgent need for NIST to issue

Comment Number: 061	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

recommendations based on strong privacy principles that can be reflected in these technical standards and requirements.

Rationale/Recommendation

Adopting a “privacy by design” approach, and building standards that reflect privacy interests, rather than attempting to tack on privacy at a later point, is the most effective means of protecting consumer privacy and security. Embedding privacy protections into the technology now, before smart meters and other Smart Grid technologies are fully deployed, and as information systems are being developed, will also be less expensive than attempting to address these issues in the future, and will make the grid more adaptable to changing threats to privacy and security as use increases.

Further, ensuring that a robust set of privacy principles underlie NIST’s Smart Grid framework is important in providing guidance to state regulators, utilities, third-party service providers, and device manufacturers wrestling with privacy issues. California, for example, recently amended its Public Utility Code to require the Public Utility Commission to explicitly consider NIST standards as a candidate for implementation in the State’s Smart Grid infrastructure. We commend NIST’s efforts to date to consider the privacy implications of the consumer-to-utility information collection envisioned in the Smart Grid, and especially the work of the Cyber Security Coordination Task Group (“CSCTG”) in performing an initial Privacy Impact Assessment (“PIA”) of that collection in the Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements document (“Draft”). However, much work remains to be done. Developing effective privacy protections for the Smart Grid must be grounded in a rigorous examination of how the proposed technologies will affect consumer privacy interests. In this Comment, we provide an overview of consumer data flow in the Smart Grid under several standards identified by NIST for implementation, discuss the privacy risks and legal rules implicated by these technologies, propose a specific framework for further developing privacy protective principles that should be reflected in the technical standards and requirements ultimately recommended by NIST, and call for the rigorous development of relevant use cases that can inform standards bodies and technology design. While our Comment generally addresses the standards proposed in the NIST Draft Framework and Roadmap, 1.0 (“Framework”), we focus specific attention on the discussion of consumer privacy and applicable principles in Chapter Two of NISTIR 7628, "Privacy and the Smart Grid."

Disposition

Organizations utilizing the Smart Grid should take a holistic view towards privacy, building in privacy from project initiation whenever possible, rather than as an add-on at a later date. The Privacy sub-group plans to develop relevant use cases with the intent of including them in the final version of the NISTIR. The second draft of the NISTIR includes

Comment Number: 061	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	suggested privacy practices that are applicable to the Smart Grid that may be useful to many organizations.	

Comment Number: 062	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	We appreciate NIST's recognition that for customer-to-utility data flow, "the specific data items involved, and associated privacy issues, are very different" from the types of data flows between commercial meters and utilities. In this section, we review and summarize data flow in the Smart Grid that implicates consumer privacy, especially consumer privacy within the home, and that is either presently covered by standards identified for implementation by NIST, or available in representative products and services currently on the market. While we cannot be comprehensive, this data flow analysis conveys a basic picture of Smart Grid data flow, as implemented in existing standards and technologies. Currently, smart meters comprise about 4.7%, or 6.7 million, of all electricity meters in the U.S., and the Department of Energy projects that 52 million more smart meters will be installed by 2012. Using stimulus funds allocated to the modernization of the electrical grid, the Administration recently announced Smart Grid grants of $3.4 billion dollars to fund the implementation of smart meters in 18 million homes. At the same time, manufacturers are working to roll-out "smart" versions of household appliances over the next several years, which will be capable of communicating with smart meters and other appliances, and directly with utilities in some instances. In addition, consumers can purchase and install their own metering devices that monitor energy consumption of a home or an individual device in close to real time. As widely noted, Smart Grid technologies have the ability to collect far more detailed information about consumers than previous systems. This enhanced access to consumption information promises several benefits: it allows consumers to track their energy use at different times of the day, and enables utilities to implement time-of-use pricing, whereby consumers are charged higher prices for energy during peak demand periods and charged less when energy demand is low. In response, consumers can defer their energy consumption from peak demand periods to a later hour. This "demand response" process improves energy efficiency by reducing peak demand, and at the same time, may reduce consumer's energy bills. Other major benefits of the transition to the Smart Grid, not directly related to consumer information, include reducing greenhouse gases by allowing the efficient use of clean energy sources and enhancing grid defenses against attack and outage.	

Comment Number: 062	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

The increased flow of data related to customers' homes in the Smart Grid exemplifies a paradigm shift from the traditional customer-to-utility data flow. First, the Smart Grid entails much more granular data collection compared to historical practice— all Smart Grid technologies contemplate or actively rely on the collection of energy consumption data at much shorter time intervals than historically collected from household consumers, down to real-time or near real-time. Second, Smart Grid technologies may allow utilities to collect electricity consumption data for a single, uniquely identified home appliance, while historically, utilities have only collected aggregate electricity consumption data of all appliances within a household. Third, a much greater variety of information is collected by Smart Grid technologies than has been collected by conventional energy services. Utilities may collect not only energy consumption data, but also unique identifiers and functionality of home appliances, temperature inside the home, and location information of plug-in hybrid electric vehicles in the Smart Grid, just to name a few. Finally, third-party entities that will have access to customers' private data, such as Google PowerMeter and Microsoft Hohm, have entered the energy marketplace.

To illustrate these changes, consider Pacific Gas & Electric's ("PG&E") SmartAC program, in which the utility company installs programmable thermostats for consumers' air conditioners, which communicate directly with the utility. PG&E might use the communication channel to display messages on the screen of the thermostat, such as weather warnings, greetings, and system maintenance notices. Consumers can also configure their thermostats on PG&E's website, giving the utility company information about consumers' temperature preference in their homes. It is possible that utilities could use the same communication channel to collect real-time readings on the temperature of consumers' homes, which, if temperature is an indicator of presence, might reveal that residents are not home (e.g., a thermostat is left at 55 degrees in the winter for several days). If a consumer chooses to register other smart appliances or a home area network (HAN) with the utility company in order to enroll in certain utility-sponsored programs, detailed information about those appliances or the HAN could also be collected by the utility.18 Utilities may remotely turn off consumers' registered devices, or instruct consumers' devices to shed load. Furthermore, if a consumer is interested in using a third-party service to monitor usage, such as a web interface offering a visualization of energy use through a graphical display, the consumer can authorize a provider such as Google PowerMeter to collect smart meter data directly from utilities.

This paradigm shift in data flow undermines key assumptions underlying existing privacy laws and regulations and imposes considerable privacy risks on customers, as we further explore below. Privacy principles developed for the Smart Grid should be grounded in a thorough review of the data flow implicating consumer privacy, including an analysis of how consumer data is being collected, used, and retained by various entities under the standards identified for implementation. We hope the information presented in this Comment may assist NIST in that effort.

Rationale/Recommendation

Comment Number: 062	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	None	
	Disposition	
	The NIST Smart Grid Privacy Subgroup would like to thank you for addressing the issue of privacy in your reply to the NIST October 9, 2009 Federal Register Notice. We have reviewed all submissions that addressed privacy concerns. These comments were beneficial in informing and shaping our work regarding Smart Grid and privacy.	

Comment Number: 063	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	Data Flow in Standards Identified by NIST for Implementation - Under the Energy Independence and Security Act (EISA) of 2007, NIST is charged with the responsibility to “coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems.” In September 2009, NIST published its Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, which identified 31 existing standards that could be implemented in the Smart Grid. Of the standards identified for implementation by NIST, the standards related to demand response and to the Home Area Network (HAN) directly involve demand-side energy management of consumer appliances and implicate consumer privacy issues. As such, we explore some of these standards here: the ZigBee/HomePlug Smart Energy Profile, Open Automated Demand Response (OpenADR), and OpenHAN. We note that this is by no means a comprehensive list of standards that may affect consumer privacy in the Smart Grid— many other aspects of architecture and practice will be relevant, as well. We include these below because of their direct relevance to consumer interaction with the Smart Grid and their obvious implications for privacy.	
	Rationale/Recommendation	
	None	
	Disposition	
	In the next version of the NISTIR, we are going to be reviewing many standards which will include privacy issues. The security requirements will address the protection of personal information and energy usage data.	

Comment Number: 064	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2

Comment

The ZigBee/HomePlug Smart Energy Profile is jointly developed by ZigBee Alliance and HomePlug Powerline Alliance members and was selected by NIST as an interoperable standard for HAN devices and communications. It is created to “further enhance earlier HAN specifications (specifically, the ZigBee Alliance Smart Energy Profile, v 1.0)” and “serves as the basis for a following Technical Requirements Document (TRD), which is the next step in line with creating the actual specification.”Although the ZigBee/HomePlug Smart Energy Profile includes a variety of use cases and its Technical Requirements Document is still being developed, important details about its implementation can be gleaned from the ZigBee Alliance Smart Energy Profile Specification, v 1.0, upon which the ZigBee/HomePlug Smart Energy Profile is based. The information below is based on our review of ZigBee Alliance Smart Energy Profile Specification, version 1.0.

A ZigBee Smart Energy network may consist of an Energy Service Portal (ESP),

Metering Device, Programmable Communicating Thermostat (PCT), and Smart Appliance Device. The ESP serves as the gateway that connects the utilities’ communications network to the consumers’ Smart Appliance Devices. The ESP may be installed within a meter, thermostat, In-Premise Display, or as a standalone device. A consumer’s devices must join the ZigBee Smart Energy network to communicate with the ESP, other devices on the network, or the utility. Within a ZigBee Smart Energy network, the ESP communicates with customers’ devices via encrypted wireless communication.

To join a Smart Appliance Device, such as a washing machine or refrigerator, to a ZigBee Smart Energy network and communicate securely with the ESP of the network, a customer needs to register the Smart Appliance Device with the utility. The registration process requires the customer to provide the utility with the 64-bit device identifier that uniquely identifies the Smart Appliance Device, the first 24 bits of which could uniquely identify the manufacturer of the device.28 The device identifier is conveyed from the customer to the utility via an out-of-band mechanism such as a telephone call, or web site registration. The utility then uses the device identifier to create keys for secure communication between the ESP and the joining Smart Appliance Device. The device identifier may also be used by the ESP to maintain a list of authorized devices for a particular HAN.

Metering information, including electric, gas, water, and potentially thermal consumption data, of smart devices may be collected by the ESP and potentially revealed to the customer’s utility. Metering Devices may be fitted with Smart Appliance Devices, and measure energy usage at the device level. In the design of ZigBee Smart Energy Profile Specification, Metering Devices and Programmable Communicating Thermostats (PCT) are all directly connected to the ESP. Since the ESP is often embedded in smart meters that communicate with the utilities, utilities could easily obtain metering information from Metering Devices or PCTs, revealing the energy usage of individual Smart Appliance Devices or the temperature inside customers’ homes.

Comment Number: 064	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

	The demand response and load control commands in the ZigBee Smart Energy Profile Specification could reveal the functionality of customers' Smart Appliance Devices. The ZigBee standard defines 12 Device Classes, including water heater, interior/exterior lighting, electric vehicle, and spa. Each Smart Appliance Device is assigned a Device Class by the device manufacturer. In a demand response or load control event, a command from the utility indicates the class of devices needing to participate in the event. The Smart Appliance Device may report event participation in a unique manner as defined by the device manufacturer, or ignore the event if the Device Class of the Smart Appliance Device does not match the Device Class in the command. Therefore, utilities could easily identify the Device Class of a Smart Appliance Device inside a customers' home from the response the utilities receive to demand response and load control commands. For instance, if a utility sends a load control command indicating a customer's water heater needs to "reduce its average load by 10 percent" and receives a response from the customer's ESP confirming participation in the event, the utility could easily tell that the customer has a water heater. As such, technologies developed under the Zigbee standard could collect and communicate far more detailed information than has been collected in the past, and use of these technologies could result in information about the intimate life of a household leaving the home and being stored outside of it, in utilities' or other providers' systems.
	Rationale/Recommendation
	None
	Disposition
	In the next version of the NISTIR, we are going to be reviewing many standards which will include privacy issues. The security requirements will address the protection of personal information and energy usage data.

Comment Number: 065	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Overall	Comment
	The Open Automated Demand Response Communication Specification (OpenADR), developed by Lawrence Berkeley National Laboratory, is a communications data model designed to facilitate automating demand response actions at the customer location. OpenADR has been used in over 200 facilities in California41 and has been identified by NIST as one of the Smart Grid standards available for implementation. In contrast to the ZigBee/HomePlug Smart Energy Profile, which aims to enable "communication between utility companies and everyday household devices," OpenADR was initially developed to "provide interoperable signals to building and industrial control systems" and is

Comment Number: 065	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

currently used by large businesses in California with centralized energy management systems. However, OpenADR has also been successfully deployed in residential settings and Programmable Communicating Thermostats (PCTs) are being developed to allow residential facilities to participate in OpenADR programs.

In the OpenADR architecture, the Demand Response Automation Server (DRAS) is the intermediary for the communication between the utility and consumer. The DRAS may be a standalone third-party service, or integrated with the utility or consumer's information system. A DRAS Client is a device on the customer's premise that communicates with the DRAS. OpenADR mandates that all public communication interfaces be subject to confidentiality, integrity, authentication and non-repudiation requirements, and has identified a minimum level of cipher suit for DRAS, which includes standards for key exchange, data encryption, message integrity and message authentication. The OpenADR identifies its opt-out functionality as one of its defining features, and requires that customers can opt out of a demand response program at any time.

The OpenADR standard contains seven use cases, and each use case covers three broad scenarios: configuration, execution, and maintenance. For our purposes, we extract one-directional customer-to-DRAS, DRAS-to-utility, and customer-to-utility data flow from the use cases and scenarios. Customers, or the DRAS Client on a customer's premise, provide the following information to the DRAS:

- Configuration information used to set up a connection with the DRAS, including identification and password of the customer and the DRAS Client, IP connection information, and the customer's contact information.
- Customer's bid for load reduction, if the customer participates in the utility's bidding program. After the customer receives a request for bids from the utility, the customer may submit a bid to the DRAS. Customers may adjust or cancel their current bid.
- Feedback information from the DRAS Client to the DRAS when a demand response or bidding event is executed. The feedback information includes customer ID, near-real-time load, amount of load reduction, and load reduction end uses (e.g. HVAC or lighting).
- Optionally, the load reduction potential of the customer.

The DRAS provides the following information to the utility:

- Customer's standing bid, if the customer participates in the utility's bidding program.
- Feedback information from the DRAS Client.
- Optionally, load reduction potential based upon all customers in program.

The utility also measures customers' electricity usage, but the details of the process are beyond the scope of the OpenADR standard.

Comment Number: 065	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	Under the OpenADR standard, utilities do not interact directly with customers' HAN devices, but interact with customers' energy management system. This design has three implications: first, to use OpenADR, customers must have their own energy management system that translates demand response signals from utilities to actionable instructions for Home Area Network devices (HAN devices). Second, utilities collect far less information about customer's devices under OpenADR than under the ZigBee Smart Energy Profile Specification. For instance, customers do not need to register their HAN devices with utilities, since the utilities do not directly communicate with customers' HAN devices but with customers' energy management systems. Third, utilities exert less control over customers' HAN devices. For instance, instead of a command instructing customers' water heaters to reduce load by 10%, as is contemplated by the ZigBee Smart Energy Profile Specification, an OpenADR command would only instruct a consumer's energy management system to reduce load and then the consumer's energy management system would decide how to respond.	
	Rationale/Recommendation	
	None	
	Disposition	
	In the next version of the NISTIR, we are going to be reviewing many standards against security requirements included in the NISTIR.	

Comment Number: 066	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	The OpenHAN standard identified by NIST for implementation is the collaboration of more than a dozen investor-owned North American utilities and reflects utilities' view of the Home Area Network. It is a high-level policy statement rather than a requirements document. Similar to the ZigBee Smart Energy Specification, OpenHAN has use cases in which a HAN device is registered with the utility and communicates with the utility via the Energy Service Interface, which may be embedded in smart meters. In addition, OpenHAN has also included an Energy Management System (EMS) that receives notification from utilities and controls connected HAN devices. The EMS may be offered by third parties; however, the utility may still require HAN device registration in the Energy Management use case for reliability programs, according to OpenHAN.	
	Rationale/Recommendation	

Comment Number: 066	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	None	
	Disposition	
	In the next version of the NISTIR, we are going to be reviewing many standards against security requirements included in the NISTIR.	

Comment Number: 067	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	We provide here some background on the role third party service providers are likely to play in the collection and use of consumer energy data in the Smart Grid. These products mainly include third-party web portals, consumer devices and Home Area Network vendors. Third-party web portals, such as Google PowerMeter and Microsoft Hohm, collect customers' smart meter reading data. Third-party web portals may enter into partnership with utilities, and obtain customers' smart meter reading data from the utilities. The frequency of these readings may depend on customers' utility. Third-party web portals may also obtain customers' meter reading data from metering devices that customers purchase. For instance, one of Google PowerMeter's device partners, a company called TED (for "The Energy Detective"), uses "clip-on current transformers" that can measure electricity consumption of a home, or an individual device, with accuracy within 2%. The electricity consumption data is collected in real-time and relayed to a customer gateway device via ZigBee wireless communication. The customer gateway device then provides the data to a stand-alone device or computer to be displayed to the customer, or provides the data to Google PowerMeter every 10 minutes if the gateway is connected to the Internet. Third-party web portals may also solicit customers to provide information about their homes via the web portal. For example, Microsoft Hohm encourages customers to provide detailed information about their home in order for Hohm to make energy-saving recommendations to customers. Information that Hohm solicits includes the heating system of customer's house, the number of occupants, and materials used for walls and floors. Although third-party web portals will have access to, store and use highly revealing customer data, they may not be held to the same confidentiality requirement as the utilities from which the third-party web portals obtains the data, as we will further explain in Section III.B. The market for Home Area Network (HAN) devices and services is still nascent but rapidly evolving. Some vendors offer consumer-oriented devices such as programmable thermostats and in-home displays, while other	

Comment Number: 067	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

	vendors provide comprehensive solutions to utilities with HAN as a part of the overall solution. For instance, one vendor, Tendril, has developed a system, called Tendril Residential Energy Ecosystem (TREE) that implements the ZigBee Smart Energy Profile. The TREE system includes data management, data transmission and demand response solutions for utilities, as well as a web portal called Vantage that provides utility customers the tools for HAN registration, device management, consumption data monitoring, etc.
	Rationale/Recommendation
	None
	Disposition
	In the next version of the NISTIR, we are going to be reviewing many standards against security requirements included in the NISTIR.

Comment Number: 068	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2	Comment
	Implications of Smart Grid Data Flow for Consumer Privacy - The details of data flow in the Smart Grid, as explored above, provide an important foundation for understanding a range of customer privacy and security issues created by an interconnected digital grid. While the wealth of information collected by Smart Grid technologies provides significant benefits to consumers, it also presents new privacy risks. The unprecedented amount of information collected about customers' energy and appliance use has the potential to reveal intimate details about daily lives and activities inside homes. These risks are compounded by the lack of a clear framework or rules to apply to the new technology landscape, which we discuss below.
	Rationale/Recommendation
	None
	Disposition
	We recognize that the Smart Grid can introduce new privacy risks and are making recommendations on how to address these risks.

Comment Number: 069

Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang

Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2

Comment

Customer Data Concerning Home Activities Presents Privacy Risks That Must Be Addressed - Our review in Section II comprises a partial picture of the great variety of information about customers' homes that is or could be collected by various Smart Grid technologies and practices. Such information may include device identifiers that uniquely identify a smart device and the manufacturer, control signals that reveal the function of smart devices, energy consumption at frequent time intervals at both the household and device level, temperature inside customers' home, status of smart devices such as IP address and firmware version, and customers' geographic region.

In addition, with the rapid development of analytical software, consumption data,either taken by itself or combined with other information, may be used to infer even more details about customers' lives inside their homes. For instance, even if energy consumption is not collected for individual appliances, information about energy consumption of individual appliances can be reconstructed from aggregate smart meter reading data of a household by using non-intrusive appliance load monitoring ("NALM") techniques. Researchers can compile libraries of appliance load patterns and match similar patterns in the time series data of overall utility usage records. Research shows that analyzing fifteen-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances. As the time intervals between data collection points decreases, home appliance use will be inferable from overall utility usage data with greater and greater accuracy.

The great variety of information about customers' homes being collected or likely to be collected, as well as analysis of that information, gives rise to serious privacy concerns. Home appliance use reflects intimate details of people's lives and their habits and preferences inside their homes. As Justice Scalia recognized in Kyllo v. United States, "at what hour each night the lady of the house takes her daily sauna and bath" is "a detail that many would consider 'intimate.'" Some of the activities that might be revealed through the Smart Grid include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, and activities that signal illegal, or simply unorthodox, behavior. As a result, information collected by the Smart Grid is valuable for many purposes other than energy efficiency, most prominently commercial exploitation by advertisers and marketers, access by criminals who wish to peek into homes, and access to household information and surveillance by law enforcement, as discussed further below.

In identifying standards and making recommendations for technology design and service deployment, NIST should consider what uses of this information may emerge that could have an adverse impact on consumers, invading the traditionally protected zone of the home and home life. Without planning, such adverse impacts could drive opposition to the Smart Grid and prompt a backlash against data collection that could be socially beneficial when limited to the narrow purposes of improving efficiency. For example, much of the information collected by the Smart Grid about customers is commercially valuable, and could be resold for a profit. In other contexts, companies have repurposed

Comment Number: 069	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

information in ways that are beyond the bounds of consumer bargaining or expectations.

Because of the intimacy of home life, data collected by Smart Grid technologies and services could be put to especially trangressive purposes. For example, an analysis of smart meter data revealing customers' home activities and daily routines could be commercially valuable to life insurance companies looking to adjust rates for customers with purportedly unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in their customers' energy usage records to verify whether the customers are actually living in those houses. Advertising companies offering behavioral targeting products might wish to enhance existing customer profiles with energy usage data revealing customer activities and habits, following a recent trend in the merging of online and offline data sources to support more targeted third-party advertising. As explained in Section II, device identifiers and control signals reveal to the utilities the manufacturers, functionality, and usage of smart devices, which is valuable for the market research and marketing efforts of smart appliances manufacturers and others who wish to target particular demographic groups. Data brokers, advertisers, marketing research firms, and others might also find this type of detailed information about customer habits attractive.

Criminals might also seek access to smart meter reading data or other information collected by the Smart Grid, in hopes of using this data to infer whether anybody is present in a house and to determine the most desirable time to commit a crime. In addition, because the Smart Grid enables the accumulation of personally identifiable and other revealing information over long periods of time, information-gathering via Smart Grid technologies could reveal behavior patterns likely to be repeated in the future, allowing criminals to plan for future attacks. If personally-identifying information accumulated by the Smart Grid is accessible to computer hackers or to "war drivers" monitoring a wireless network, the information could also be used by criminals to commit identity theft, especially when utilities or other providers use unsecured paths to transmit data. For instance, many businesses and others traditionally use energy consumption data to authenticate customers, making the information particularly valuable to those attempting illicitly to take over someone else's account. Threats to customer data security are compounded if the data transmission within Smart Grid networks is not encrypted, in which case criminals may be able to easily intercept Smart Grid transmissions and acquire the content of communications.

For a variety of reasons, law enforcement officials may also be interested in the fine-grained data about household habits collected by the Smart Grid. As part of their investigatory work to solve crimes, officials may want to establish or confirm residence at an address at a certain critical time, and this information may be gleaned from smart meter reading data or temperature inside the home collected by a programmable thermostat. Law enforcement may also be interested in data collected by the Smart Grid that indicates illegal or other activities at home. For instance, access to smart meter reading data might be used in drug investigations, to enable law enforcement to learn about a suspect's marijuana growing cycle. The data from Smart Grid technologies certainly may be highly useful for these purposes. At the same time, the privacy implications of law enforcement officials' interest in obtaining smart meter data suggest the

Comment Number: 069	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

	need for strong Fourth Amendment procedural protections for this information, as well as careful procedures on the part of utilities and other providers, and technology design that allows for strong data protection. Already, a California family was put under surveillance by law enforcement for having an unusually high electricity bill, which turned out to merely reflect the legitimate activities of a busy household. Procedural safeguards may be especially important in light of the fact that Smart Grid data held by third parties as business records may not be subject to the same protections applicable to information kept within the home.
	Rationale/Recommendation
	None
	Disposition
	We have included recommended privacy practices in the second draft of the NISTIR. Also, the chapter has been significantly revised and includes a discussion of many of the topics listed above.

Comment Number: 070	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2	Comment
	Under longstanding U.S. constitutional values and law, activities occurring within the sanctity of individuals' homes, because of their inherently personal nature, have been afforded special protection from intrusion by others.91 The Supreme Court recently affirmed this strong protection for all types of data found in the home, noting in Kyllo v. United States that the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained…in the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes." In Kyllo, the Court invalidated the warrantless use of thermal imaging technology to measure heat emanating from a home as an unlawful search under the Fourth Amendment, despite the lack of any physical intrusion into the home by law enforcement. Data collected via Smart Grid technologies are similarly revealing of the intimate details of home life, and should be subject to similarly high levels of protection. At the same time, the customer data collected and used in the Smart Grid is governed by a patchwork of broad state and federal laws that may be generally applicable, but those often neither specifically address the electrical grid nor were developed with Smart Grid technological advancements or business models in mind. In addition, at present, there is no federal customer privacy law in the U.S. that might generally cover commercial activities related to Smart Grid information.

Comment Number: 070	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

We appreciate NIST's recognition that a "lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed." Rather than falling under a comprehensive single law, the Smart Grid intersects with a number of different federal and state rules regarding the privacy of activities occurring within the home, the handling of business records and identifiable customer information, the privacy of electronic communications, and access to computer systems. Neither in isolation nor taken together do these existing laws provide adequate protection for the categories and quantities of data that may be generated by the Smart Grid. As such, technology design and utility and third-party service provider practices must be carefully considered and rigorously implemented in order to protect customer privacy and security.

Historically, the principal source of privacy regulation for electricity data has been state public utility commissions, which place varying restrictions on consumer energy data. In some states, utilities may provide competitive suppliers access to customer energy data without the ratepayer's affirmative consent. While other state public utility codes place explicit restrictions on the sharing of customers' personal information, these rules contain some regulatory uncertainty as to their coverage of some types of Smart Grid data. And generally, state utility commissions are just beginning to consider the privacy implications of Smart Grid data. General state laws governing business' and third parties' collection and use of customers' personal data may apply to energy usage, but may be too narrow to cover the extensive and varied information generated by the Smart Grid, or the increasing number of entities that have access to the information. For example, California Public Utility Code Section 4.4 imposes a general requirement on electric service providers to ensure confidentiality of customer information, However, the emergence of third-party service providers such as Google PowerMeter and Microsoft Hohm means that new entities have access to customers' private data, but likely stand outside the statutory confidentiality requirement because they are not "electric service providers" under California law. Furthermore, new types of information, such as the unique identifiers of smart devices collected by the utilities, create uncertainties about whether current privacy law could be extended to these new types of information. It is also important to note that California has a relatively protective regime for personal data and other states' privacy regulations may vary greatly in terms of the rules governing utilities and third party service providers.

At the federal level, there is a similar patchwork of rules, which provides even less directly relevant guidance on the privacy protections applicable to the Smart Grid. The Electronic Communications Privacy Act (ECPA) sets out limitations on the interception of electronic communications and has been broadly applied to a range of communications systems. However, one of the greatest privacy concerns for consumers is what the utilities will do with information they receive from their customers, and ECPA places no limit on that. The FCC's Customer Proprietary Network Information (CPNI) Rules, which require telecommunications carriers to obtain customers' opt-in before using,

Comment Number: 070	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	disclosing, or permitting access to individually identifiable customer information, do not necessarily directly bear on the privacy issues surrounding a Smart Grid information network. However, as the transmission of Smart Grid services grows increasingly complex and more communications-based, utilities may find themselves subject to laws governing telecommunications providers, meaning they would be bound by some privacy protections on data related to their service. The Computer Fraud and Abuse Act (CFAA), which governs unauthorized access to computer systems, may also be relevant, under a broad construction, to regulate invasions of the Smart Grid. Unauthorized access to obtain information from or cause damage to devices like smart meters, wireless sensors, smart appliances, and a customer's home computing system might generate liability under an expansive reading of the CFAA. Finally, the Federal Trade Commission (FTC) likely has general jurisdiction under Section Five of the FTC Act to pursue actions against Smart Grid entities engaging in "unfair and deceptive trade practices," such as, for example, failing to adopt, disclose, or adhere to reasonable privacy and security practices. This brief and introductory discussion of the rules possibly applicable to Smart Grid technologies reveals the disjointed and outdated nature of current customer protections for energy data. Industry lacks a clear set of privacy guidelines to govern Smart Grid technologies. In light of the legal patchwork, we are especially in need of a cohesive approach that reflects the realities of an interconnected and digitized electricity grid in which customers are active contributors of personal data.	
	Rationale/Recommendation	
	We encourage NIST to include in its Framework comprehensive privacy principles against which technical standards can be evaluated to ensure that both Smart Grid technologies and service providers are sufficiently protective of consumer privacy.	
	Disposition	
	We have included recommended privacy practices in the second draft of the NISTIR. Also, the chapter has been significantly revised and includes a discussion of many of the topics listed above.	

Comment Number: 071	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	Proposed Framework for NIST Privacy Principles - The discussion of unique risks to privacy presented by the Smart Grid, and the present lack of comprehensive legal rules mitigating those risks, reveals the need to develop strong design and business practice mechanisms for protecting consumer privacy in the modernized grid. In the	

<table>
<tr><td>Comment Number: 071</td><td>Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang</td><td>Comment Type: __ Technical __ Editorial _X General</td></tr>
<tr><td rowspan="5"></td><td colspan="2">following section, we lay out the necessary elements for developing a comprehensive framework to protect privacy in the Smart Grid, including who should be covered, what types of data should be included, and how principles can ensure the fullest protections for consumers' Household Energy Data.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">All of the technical standards identified by NIST for implementation in the Smart Grid should be evaluated against these principles, and ultimately, the Framework for standards and requirements released by NIST should reflect these principles.</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">Thank you for the suggestion. We will consider this in subsequent versions of the NISTIR.</td></tr>
</table>

<table>
<tr><td>Comment Number: 072</td><td>Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang</td><td>Comment Type: __ Technical __ Editorial _X General</td></tr>
<tr><td rowspan="4">Reference: Chapter 2</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">Ensuring that the full range of companies touching consumer data in the Smart Grid are covered by any privacy protections is critically important. In the current NIST Draft, the examination of privacy risks and potential safeguards in Chapter Two focuses too narrowly on "consumer-to-utility" data flows. Instead, the activities of utility companies, third party service providers, such as Microsoft and Google, and device manufacturers, such as General Electric and Honeywell, in collecting, using, and storing consumer data should all be considered, and technical standards should be evaluated in light of known business practices and service models in addition to technology capabilities. Privacy principles should not subject different entities to a different set of rules where the entities are similarly interacting with consumer data. Furthermore, recognizing this universe of participants now is important in fully incorporating "privacy by design" into the applicable standards and technologies underlying the Smart Grid.
In performing an evaluation of the proposed standards, a well-developed set of use cases explaining how privacy principles should be built into the Smart Grid will be important in ensuring the full implementation of consumer privacy protections.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">Privacy Principles Should Cover All Smart Grid Entities and Practices. For the final Framework, NIST should develop use cases that reflect a comprehensive model of data flow, covering all entities and activities, and detail the</td></tr>
</table>

Comment Number: 072	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	necessary consumer privacy protections which should be required in all Smart Grid standards and technical requirements.	
	Disposition	
	We have revised this section acknowledging that there will potentially be more than utilities that are participating in the Smart Grid environment.	

Comment Number: 073	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	Designing an effective framework to protect consumer data also requires specific consideration of what information requires protection. As drafted, the privacy principles in the NIST Draft are built upon the model of “personally identifiable information” (“PII”), including the “notice and purpose for PII use,” “collection of PII,” and the “use and retention of PII.” In the context of the Smart Grid, however, the privacy assessment of consumer data practices must extend beyond traditional notions of PII, which has a longstanding history of special legal consideration for its ability to directly identify an individual, such as a name, address, email address, or phone number. Certainly some of the data collected by utilities and third party service providers in the Smart Grid, such as name and address for billing purposes, would be considered PII under traditional definitions. But based on the discussion of consumer data flow described above in Section II, it is clear that some data collected and used in the Smart Grid extends beyond traditional PII, yet is very revealing of traditionally protected household activities and intimate home life.	
	Rationale/Recommendation	
	We recommend that NIST adopt privacy principles that cover a somewhat broader set of intimate information: “Household Energy Data.” Household Energy Data includes: any consumption or device data capable of revealing personal or household information that is not aggregated over long periods of time or over a large number of ratepayers. Specifically, Household Energy Data includes both: a. traditional PII, such as account information used for billing purposes and unique device identifiers tied to an individual name, which is either immediately personally identifiable or becomes personally identifiable when combined with other collected information; and	

Comment Number: 073	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

b. data collected about an individual household in the Smart Grid that is revealing of home life by itself or when analyzed or combined with other information. Examples of this second category of Household Energy Data include: near real-time energy usage data, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering data (e.g. thermostat temperature).

Sometimes information in the second category will be personally identifiable when combined with other types of information, or when the number of people in a household is small, while sometimes it is unlikely to identify individual members of a household, at all. Regardless of whether it is identifiable, however, it is inherently revealing of household activities and home life, traditionally private domains that are, and should continue to be, protected from observation. While not all Household Energy Data may uniquely identify an individual in a multi-person household, it can still reveal highly personal and invasive details about daily activities of people living in the home, such as the use of a specific medical device or an absence from the home, raising the serious privacy issues explored above. Further, given that 32.2 million people live alone in the U.S and twenty eight percent of American households have single-person occupancy, Household Energy Data is revealing of individual activity for a significant number of Americans.

Examples of data not covered by "Household Energy Data" include usage records aggregated in 30-day increments—what is collected now through monthly metering readings—and other types of data aggregated across a large number of households. While still needing some safeguards, such data likely does not require the full scope of protections outlined here.

We also note that this working definition of Household Energy Data, and the following discussion of a privacy framework to protect this data, is intended to be a baseline for the least revealing information included within the definition. Some of the information included within the set of "Household Energy Data," such as PII and location-identifying information will likely require additional protections. The principles discussed here for Household Energy Data outline the minimum protections required for this basic category of data.

Disposition

We agree the term PII is too narrow and have used the term personal information. Also, the chapter has been significantly revised and includes a discussion of many of the topics listed above.

Comment Number: 074	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference:	Comment	

Comment Number: 074	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Chapter 2	Privacy Principles for Household Energy Data Should be Grounded in Comprehensive Fair Information Practice Principles (FIPPs) - Here, we consider the larger question of how to protect the Household Energy Data collected and used in the Smart Grid. Properly formulated and rigorously implemented Fair Information Practice Principles ("FIPPs") provide a broad, comprehensive privacy framework that should underlie privacy standards for the Smart Grid. We urge NIST to adopt appropriately formulated FIPPs as the basis for its consumer privacy recommendations. While we appreciate the Cyber Security Coordination Task Group's (CSCTG) effort to consider a set of rules extending beyond notice and consent, the privacy principles as drafted need considerably more specificity and organization. Given the broad acceptance of FIPPs by national and international privacy regulators, the fact that they have been applied in many contexts related to consumer privacy, and the fact that the lesser-known Generally Accepted Privacy Principles (GAPP) cited in the NIST Draft are grounded in FIPPs, it is most sensible to revise the Draft's privacy principles to more fully reflect FIPPs.	
	Rationale/Recommendation	
	In particular, the technical standards and requirements ultimately recommended by NIST should incorporate FIPPs, and should recommend that relevant technologies be designed to have the capacity to implement FIPPs, and to interoperate based upon them, enabling "privacy by design." While various versions of FIPPs are used by different regulatory bodies, we consider here, and recommend for adoption, the articulation of FIPPs in the Department of Homeland Security's (DHS) 2008 Privacy Policy memorandum. Compared to prior versions of FIPPs, that sometimes provided vague, incomplete, and generally weakened privacy protections, the DHS framework is the U.S.-based framework that most closely follows strong international interpretations of FIPPs. It provides a robust set of modernized principles that NIST should apply to all entities collecting consumer data in the Smart Grid.	
	Disposition	
	FIPP was one of the sources that was used to develop the privacy principles of the second draft of the NISTIR.	

Comment Number: 075	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	Transparency: Smart Grid entities should be transparent and should provide meaningful, clear, full notice to the individual regarding the collection, use, dissemination, and maintenance of Household Energy Data.	
	Rationale/Recommendation	

Comment Number: 075	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Relevant information about the collection, use, dissemination and maintenance of Household Energy Data must be shared with the consumer. This information-sharing must extend beyond mere notice of collection practices; it must also include providing consumers with clear, detailed information about the specific uses of their data, retention periods, and any transfers of data to or access by other entities. Notices should state clearly: what information is collected, whether this information is shared and with whom it is shared, the period that data is retained, and the contact information for an official at each company responsible for the policy and for personal data collected by the system. For example, device manufacturers should clearly provide notice of any transfer of data, such as device status being transmitted from the device to the manufacturer, which might occur with the consumer's use of a device. Further, Smart Grid entities, including utilities, third-party service providers, and device manufacturers, should also provide consumers with access to the personally identifying information collected about them, as well as Household Energy Data collected about their homes.

Disposition

The principles and the suggested privacy practices have been revised in the second draft of the NISTIR.

Comment Number: 076	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2

Comment

Individual Participation: Entities should involve the individual in the process when using energy information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of Household Energy Data. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of Household Energy Data.

The NIST draft recognizes that "new smart meters create the need for utilities to give residents a choice about the types of data collected," but consumer choice must also extend to the use, transfer, and maintenance, including retention, of Household Energy Data. To fully recognize the principle of individual participation, Smart Grid entities must respect the range of consumer preferences with respect to their data that will exist at multiple points along the data path.

Initially, consumers should be required to opt in to the collection and use of Household Energy Data for any secondary purposes beyond what is strictly required for the provision of service. Without affirmative consent by the consumer, any use of data by utilities or third party service providers should be limited to purposes related to the original mission of the service or application. The opt-in consent should allow the consumer to exercise a genuine

Comment Number: 076	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

	choice, meaning that it does not present high practical barriers or costs if the consumer chooses not to opt in.
	Rationale/Recommendation
	In the case of utilities, this means that opt-in consent would be required for a utility to use Household Energy Data for delivering advertisements to its customers, which is clearly unrelated to the primary purpose of providing energy service. A third party service provider's use of device identifiers for marketing purposes is another example of using data for a secondary purpose. As explored further in the Use Limitation principle, NIST should develop use cases that provide specific guidance on what constitutes acceptable primary and secondary purposes of data use in the Smart Grid. Informed consumer consent should also be affirmatively required for any access to or transfer of Household Energy Data to or by third party service providers. At all points, consumers should have reasonable access to the Household Energy Data that utilities or third-party service providers are collecting and using, with mechanisms available to correct data where it contains inaccuracies and to actively manage secondary uses. There should also be parity in enrollment and any opt-out/opt-in mechanisms. That is, if an individual or household can enroll in data sharing online, they should also be able to cancel that sharing and exercise other choices about their data through the online mechanism.
	Disposition
	The privacy section has been revised to include addressing concerns for "consent" (opt-in/opt-out). Third-party data access security requirements are currently being evaluated for the next version. Note: ASAP-SG is developing a draft set security profile for Third-party Data Access. Future versions of the NISTIR may include reference to these works.

Comment Number: 077	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2	Comment
	Purpose Specification: Companies should specifically articulate the purpose or purposes for which Household Energy Data will be used. The specification of purpose should fully describe both primary purposes of data use by the utility or service provider, and any secondary purposes, as described above. Consumers should be provided with this information about how their data will be used before the time of collection by service providers. The NIST Draft allows for

Comment Number: 077	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

disclosure “at the time of collection,” but that may not provide consumers with the necessary opportunity for individual participation, which includes sufficient opportunity to separately opt in to any use of their Household Energy Data for secondary purposes.

Clearly articulating the purpose of data use enables the consumer to make an informed choice before deciding to share data. In the context of the Smart Grid, for example, one would expect a utility to specify to a consumer that “Household Energy Data” will be used for the primary purposes of providing time-of-use pricing that may reflect discounted rates during certain times of the day. A third-party service provider offering consumers an online interface for monitoring energy consumption may specify that Household Energy Data will be used to target product advertisements to the consumers (which, again, is likely the use of consumer data for a secondary purpose, requiring affirmative, additional consent). If the utility later changes the purpose for which the Household Energy Data is used, consumers should also opt in to that new use.

Rationale/Recommendation

None

Disposition

The principles and the suggested privacy practices have been revised in the second draft of the NISTIR.

Comment Number: 078	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Chapter 2

Comment

Data Minimization: Only data directly relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as necessary to fulfill the specified purpose.

Generally, Smart Grid technical standards should support, and technologies should be capable of, appropriate data minimization. In the context of the utility, the Data Minimization principle means that utilities’ collection of data for the primary purpose of providing energy use should be limited to that information necessary for billing, load management and some demand response programs—information that is “directly relevant and necessary” to the provision of the primary service. As the NIST Draft importantly notes, “only the minimum amount of data necessary for utility companies to use for energy management and billing should be collected.” Further explanation of the specific types of information necessary for utilities to perform these functions in a data minimizing manner should be detailed in the set of use cases developed by NIST, as suggested above. At the outset, we note that it is unlikely the utilities

Comment Number: 078	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

need to collect information about the functioning of individual appliances, or even individual houses, to implement load management or demand response programs.

Centralizing the collection and usage of Household Energy Data at the Smart Meter level would also enable such minimization. As smart meters become capable of more sophisticated computation, they should be engineered so that it is possible to aggregate the collection, use, and storage of private data at the point of consumption. Such a meter would aggregate and anonymize usage records over both time sequence and type of appliance so as to report only relevant abstractions of data such to the utility. It would also enable consumers to have their smart devices communicate securely with the HAN or other gateway without revealing the details of their smart devices, or the time of use, to the utility. Designing smart meters and other devices to preserve privacy by default enables households to fully participate in the decision to share their Household Energy Data outside of the home. Minimizing the data that leaves the home is especially important because of the well-established constitutional protections for data residing in the home, as discussed earlier.

While there are some likely consumer advantages tied to sending Household Energy Data to the utility (e.g. a utility may offer price discounts for consumers who share data beneficial for load research), our initial research suggests that the efficiency benefits of the Smart Grid can be realized without centralizing all control of Household Energy Data at the utility. Existing meters should be updated where possible within technological constraints, and new meters should be designed, so that consumers can choose to minimize the sharing of Household Energy Data with utilities or third-party service providers. Meters with sufficient processing and storage capacity to manage demand response pricing within the home are not currently being widely marketed, but advanced smart meters such as Itron’s OpenWay CENTRON meter, which has the capability for performing complex usage calculations and storing large quantities of data, already reveal that smart meters can allow for data minimization while still enabling the benefits of the Smart Grid. Where Smart Meters are already being installed without any capability for data minimization, NIST should adopt technical recommendations that provide for this option, especially since devices already in the field can be updated remotely.

Applying the data minimization principle to utilities also means that current retention periods for customer records, which currently widely reflect the industry standard of seven years, should be revised in light of the Smart Grid transition and attendant collection of Household Energy Data. Beyond the security advantages of reducing retention, shorter periods will likely yield benefits to the utilities in terms of decreased storage and maintenance costs.

Applying this principle to third party services providing consumers with web-based visual representations of home energy use, such as MS Hohm, suggests that those service providers should not collect appliance-level device identifiers (unless a purpose such as consumer marketing was specified to the consumer and opt-in consent was obtained prior to the use, per the principle above). Third party service providers should also enable consumers with the choice to end service and terminate their accounts, including the prompt deletion of any Household Energy Data

Comment Number: 078	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	retained by the utility.	
	Rationale/Recommendation	
	None	
	Disposition	
	The suggested privacy practices have been revised in the second draft of the NISTIR.	

Comment Number: 079	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	Use Limitation: Household Energy Data should be used solely for the purposes specified in the notice. Sharing of such information should be only for a purpose compatible with the purpose for which it was collected. In the case of a utility collecting Household Energy Data for the primary purpose of providing energy service to the ratepayer, access to that data should be limited within the utility to entities with a justifiable requirement to use the data for fulfilling the clearly-specified purpose, such as the billing department. Any secondary uses beyond those must be specified in advance, and should only occur with explicit consumer consent under an opt-in regime, as detailed above. For example, detailed information about a consumer's smart devices, such as a MAC address uniquely identifying the device and the manufacturer of the device, should not be used by a utility or third party service provider, unless such use was specified to the consumer, who specifically opted in to the purpose. Similarly, third party service providers should not use Household Energy Data for behavioral advertising or other marketing purposes when the primary purpose of the data collection and use specified to the user was more limited.	
	Rationale/Recommendation	
	None	
	Disposition	
	The suggested privacy practices have been revised in the second draft of the NISTIR.	

Comment Number: 080	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Overall	Comment
	Data Quality and Integrity: Companies should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Utilities and other entities handling Household Energy Data, including third-party service providers, should provide consumers with tools to correct mistakes or challenge information provided in profiles.
	Rationale/Recommendation
	The NIST Draft importantly noted this need to allow consumers to review and correct, where necessary, their information. Standards and technical requirements implemented by utilities and third party service providers, for example, should allow for easily-accessible interfaces which give consumers the opportunity to review and correct their Household Energy Data. This review provides the best means of ensuring that consumer data is accurate, which is particularly important given companies' data retention and transfer practices.
	Disposition
	As part of our assessment, we considered privacy when defining requirements for the logical interface categories.

Comment Number: 081	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General

Reference: Overall	Comment
	Security: Companies must protect Household Energy Data through appropriate security safeguards against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, and Smart Grid technologies and services must be capable of implementing these security safeguards. Reasonable security in the Smart Grid requires that any transmission of Household Energy Data must be secure and that data practices by utilities and other providers include meaningful safeguards for Household Energy Data. For example, if a communication is sent over an open wireless connection, or could otherwise be intercepted with reasonable or targeted efforts, encryption should be required, for both organization-owned infrastructure and third-party communication services.
	Rationale/Recommendation
	More broadly, technical standards identified by NIST for implementation should be reviewed and, if necessary, revised to require that smart-device communications provided by either utilities or third-party service providers are truly secure, prior to any recommendations being made. For example, contrary to the Draft's requirement that

Comment Number: 081	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
	“[d]emand response HAN devices must be securely authenticated to the HAN gateway and vice versa,” both OpenHAN and ZigBee standards presently identified as NIST standards for implementation include scenarios (in the provided background context for relevant use cases) in which smart devices respond to open radio signals to provide demand response capabilities. NIST should recommend that these standards be revised, as unauthenticated HAN devices responding to open, unencrypted signals pose a clear security risk for consumers. Further, Household Energy Data collected, used and maintained by utilities or other service providers must be stored securely, and must be maintained subject to secure data management practices. If a security or other breach results in the loss or exposure of Household Energy Data, affected customers should be notified and all reasonable steps should be taken to minimize harm to customers.	
	Disposition	
	As part of our assessment, we considered privacy when defining requirements for the logical interface categories.	

Comment Number: 082	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	Accountability and Auditing: Companies should be accountable for complying with these principles, should provide appropriate training to all employees and contractors who use Household Energy Data and should audit the actual use of that information to demonstrate compliance with the principles and all applicable privacy protection requirements. NIST’s current draft recognizes the importance of this principle in stating that “documented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors, and other entities with management responsibilities throughout the Smart Grid should be created and implemented, and compliance enforced.”	
	Rationale/Recommendation	
	As discussed above, an important means of ensuring widespread implementation of the full set of FIPPs is to develop rigorous, comprehensive use cases that reflect a comprehensive model of data flow as well as these principles, and that inform the development of specific privacy requirements against which companies can audit for compliance purposes. In expanding the next iteration of the Draft, and specifically in further developing the Privacy chapter, the CSCTG (now SGIP-CSWG) should develop or collect these use cases.	

<table>
<tr><td colspan="2">Comment Number: 082</td><td>Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang</td><td>Comment Type: __ Technical __ Editorial _X General</td></tr>
<tr><td rowspan="3"></td><td colspan="3">The CSCTG should also consider outlining an accountability mechanism, such as a certification programs for Smart Grid technologies and third-party services, to measure adherence to privacy principles grounded in FIPPs. Such a certification program could be helpful in establishing an industry standard for data practices by utilities or other providers that provides meaningful safeguards for the Household Energy Data. In developing such a program, California’s experience in certifying meters could be instructive.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The suggested privacy practices have been revised in the second draft of the NISTIR. Addressing a certification program will be considered for the next version of the NISTIR.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 083</td><td>Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang</td><td>Comment Type: __ Technical __ Editorial _X General</td></tr>
<tr><td rowspan="6">Reference: Chapter 2</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">As the exemplified in the prior discussion, crafting a comprehensive privacy framework for the Smart Grid is a complex task requiring the careful examination of rapidly evolving technology and business models. While well-developed tools, such as the robust articulation of FIPPs outlined here, can be quite helpful in creating privacy principles for the Smart Grid, more work must be done to apply these guidelines to modernized Grid technologies and specifically to the full set of NIST recommended standards and technical requirements that will emerge from the standards-setting process.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">As a priority for future work, we recommend that the CSCTG devote energy to developing a specific set of uses cases that reflect a comprehensive model of consumer data flow related to Smart Grid technologies and services and that are informed by the FIPPs-based framework set forth above. In addition to helping companies in the auditing process, as described above, developing a rigorous set of uses cases now will provide an important mechanism for identifying further changes that need to be made to the proposed standards to protect consumer privacy, and for evaluating where additional standards may need to be created.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The Privacy Sub-group will be developing use cases for the next version of the NISTIR.</td></tr>
</table>

Comment Number: 084	Submitted by: The Center For Democracy & Technology- Jennifer M. Urban, Elizabeth Eraker, Longhao Wang	Comment Type: __ Technical __ Editorial _X General
Reference: Chapter 2	Comment	
	Fully addressing the implications of utilities and third-party application providers' greatly enhanced collection and use of Household Energy Data in the Smart Grid may require more time than has been allocated in the current process. While we understand the tremendous interest in accelerating the deployment of Smart Grid technologies, we also strongly support NIST's observation in the Framework and Roadmap, 1.0 that the development process "must be systematic, not ad hoc." While it is certainly true that "[l]egal and regulatory frameworks can be further harmonized and updated as the Smart Grid becomes more pervasive," it is critical to develop a full, carefully considered privacy assessment now, so that the applicable standards are crafted in a way that protects consumer privacy.	
	Rationale/Recommendation	
	We suggest that the timeline for CSCTG's work be considered, and readjusted if needed, to ensure there is sufficient opportunity for a full review of these issues, including the development of the privacy use cases described above. This may require that NIST extend the target date for the completion of the final draft.	
	Disposition	
	The principles and the suggested privacy practices have revised in the second draft of the NISTIR. Recognizing the significant amount of work, we have extended the target date for version 1 of the NISTIR to spring 2010.	

Comment Number: 085	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	The government and industry should develop a higher level strategic view on Smart Grid cybersecurity issues, rather than the technical requirements set out in the current draft. The top strategic security concerns should be the integrity of communications and software; authentication and non-repudiation of information; and confidentiality of personal information.	
	Rationale/Recommendation	

Comment Number: 085	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: __ Technical __ Editorial _X General
	As these are determined, NIST should examine the design characteristics of meters, collectors, and sensors so that they would be able to support end-to-end integrity controls independent of the specific network infrastructure between them and the operations/data centers. The design requirements should also focus on making meters, collectors, and sensors easier to support and maintain over a long lifespan.	
	Disposition	
	The second draft of the NISTIR addresses all domains of the Smart Grid.	

Comment Number: 086	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X_ Technical __ Editorial General
Reference: Chapter 4	Comment	
	Both the information that flows between Advanced Metering Infrastructure (AMI) devices and the utility companies and the transport of that information require protection. The current draft tends to focus on the transport and data flow interface.	
	Rationale/Recommendation	
	NIST should also require measures to protect the information from being falsified or spoofed. The measures in the draft for AMI Message Authenticity/Integrity, such as signing and encryption, would provide significantly enhanced protection to the information that resides in various locations, such as the Supervisory Control and Data Acquisition (SCADA) servers.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document	

Comment Number: 086	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X_ Technical __ Editorial General
	which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 087	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X_ Technical __ Editorial _ General
Reference: Chapter 4	Comment	
	The Smart Grid communications flows should be kept as predictable as possible.	
	Rationale/Recommendation	
	The Smart Grid communications between the AMI meter and the utility company should not include communications from the home area network (HAN). The HAN’s untrusted environment introduces additional vulnerabilities into the communications infrastructure, and communications from HAN to the utility company should not be permitted to be sent through the meter. The AMI meter will likely have limited processing capability and not be able to provide the robust routing, filtering, and security mechanisms that are necessary to protect the communications channels and content. Nor can the utility company’s data center be expected to handle the volume of potentially threatening HAN traffic aggregated though a large number of meters. Thus, the physical separation of AMI traffic flows from non-AMI traffic is likely the best option.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 088	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	DHS-2.8.9.2 - Supplemental Guidance: The use of a third-party communication service provider instead of organization owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within an AMI system could introduce communications latency due to the additional time and computing resources required to encrypt, decrypt, and authenticate each message. Any latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the AMI system.	
	Rationale/Recommendation	
	NIST should require encryption regardless of whether the organization or a service provider is transporting the AMI messages. The AMI meter is physically present at the home and provides a readily available opportunity for mischief or malicious attack. The authenticity, integrity, and non-repudiation of Smart Grid data must be maintained from end-to-end.	
	Disposition	
	Discussions of cryptography and key management are currently being discussed within the SGIP-CSWG. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 089	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	DHS-2.8.11.2 - Supplemental Guidance: Organizations need to select cryptographic protection that matches the value of the information being protected and the AMI system operating constraints. A formal written policy needs to be developed to document the practices and procedures relating to cryptographic key establishment and management.	

Comment Number: 089	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General
	These policies and procedures need to address, under key establishment, such items as the key generation process is in accordance with a specified algorithm and key sizes are based on an assigned standard. Key generation needs to be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards.	
	Rationale/Recommendation	
	This guidance should be expanded such that all AMI devices have a unique key to identify each device. Including the same key on all devices from a single manufacturer (and separately authenticating the messages) is insufficient to protect against spoofing. Single-key schemes have been demonstrated repeatedly to be weak against cryptographic attacks.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 090	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	DHS-2.8.21.2 - Supplemental Guidance: In general, do not use domain name system (DNS) services on an AMI system. Host-based name resolution solutions are the recommended practice. However, if DNS services are implemented, it is recommended to deploy at least two authoritative DNS servers. The DNS configuration on the host will reference one DNS server as the primary source and the other as the secondary source. Additionally, locate the two DNS servers on different network subnets and separate geographically. If AMI system resources are accessible	

Comment Number: 090	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General

from external networks, establish authoritative DNS servers with separate address space views (internal and external) to the AMI system resources. The DNS server with the internal view provides name/address resolution services within the AMI system boundary. The DNS server with the external view only provides name/address resolution information pertaining to AMI system resources accessible from external resources. The list of clients who can access the authoritative DNS server with a particular view must also specify.

Rationale/Recommendation

DNS services should not be used within the AMI system. Although they are easy to use and implement, DNS services have a history of being highly susceptible to compromise. While some type of naming may be desirable (e.g., to bind a security certificate to a device name), all such devices need not perform DNS name resolution. Deploying a large number of devices with caching DNS resolvers is not advisable, particularly when alternatives, such as Dynamic Host Configuration Protocol (DHCP), secured management protocols, or IPv6 header extensions, can configure the devices at the periphery of the network, rather than having them look up names. To the extent DNS services are permitted, NIST should enhance the restriction and recommendations contained in this section to include periodic penetration-type testing for vulnerabilities, such as DNS cache poisoning in which an attacker puts a fake network address in the cache and subsequent lookups will provide the attacker's IP address, not the real address of the device. Additionally, if DNS services are approved, they must employ the security extensions commonly known as Domain Name System Security Extensions (DNSSEC). Finally, the draft should elaborate on the requirements for "host-based name resolution solutions."

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 091	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	DHS-2.12.14.1 - Requirement: The meter shall have a manual connect/disconnect switch and communication ports by which a field tool can be used to extract electric use data in the event that the communication network becomes inoperable or unavailable.	
	Rationale/Recommendation	
	The guideline should explicitly state that the “communication port” could be a wireless connection with a transmission path that is digitally signed and encrypted. Permitting wireless connections allows for future “drive-by” meter management technologies and reduces the technician time per physical location. Moreover, with a wireless connection, there is no physical port, the presence of which substantially increases the vulnerability of the device to direct physical access and attack. If a physical port is is ultimately included, it needs to be locked down.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the draft 1 of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 092	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	DHS-2.14.3.1 - Requirement: The AMI system must employ malicious code protection. Malicious code protection is important as malicious software attacks are becoming increasingly frequent. As a result, the NIST requirements should include recurring vulnerability assessments or penetration testing. Source code reviews are recommended for elements identified as critical or at high risk.	

Comment Number: 092	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X Technical __ Editorial __ General

	Rationale/Recommendation
	The AMI system must also be protected against unauthorized changes to the software in the device. In other words, it must employ some type of integrity protection or tamperproof mechanism, and be able to fail to a known state should the firmware be altered via unauthorized access.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 093	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4	Comment
	DHS-2.16.4.1 - Requirement: All AMI components must provide sufficient audit record storage capacity and capabilities to configure auditing verbosity to reduce the likelihood of such capacity being exceeded. Under normal usage conditions, components and systems must store events locally for the following minimal timeframes: 1. Embedded Devices: 1 week; 2. Traditional IT or SCADA Servers: 1 month; 3. Central Log Management Systems: 1 year.
	Rationale/Recommendation
	The current NISTIR does not include timeframes. NIST should expand the storage requirement for SCADA servers from one to twelve months. An attack that probes the SCADA environment and tests exploitability could take place over a period longer than one month and may be separated from the actual attack by more than one month. Valuable forensic information could be lost if NIST sets the retention window too narrowly.

Comment Number: 093	Submitted by: Verizon William Barns Distinguished Member of Technical Staff Network Security Architecture & Design, Network & Technology	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 094	Submitted by: GMU- Philip Sagle	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.11	Comment	
	I respectfully request that the relevant CSCTG subgroup please review the following two publications, which suggest that YASIR (Yet Another SecurIty Retrofit) and SSCP (Secure SCADA Communications Protocol) are two 'wrapper' alternatives that may answer your security and bandwidth concerns, ...and therefore may be worthy of specific mention / written-inclusion in NIST IR-7628 's next draft : YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems - http://www.ists.dartmouth.edu/library/451.pdf Hallmark Project: Commercialization of the Secure SCADA Communications Protocol, a cryptographic security solution for device-to-device communication - http://www.oe.energy.gov/DocumentsandMedia/4-Hallmark.pdf	
	Rationale/Recommendation	
	None	
	Disposition	
	Thank you for the references.	

Comment Number: 095	Submitted by: DOS- Vickie L. McCray	Comment Type: _X_ Technical __ Editorial __ General
Reference: p.C-3	Comment	
	To top of C-3 "Potential Impact" para ADD after "enforceable" add a new sentence and delete "and they must be flexible enough that they can be continuously improved."	
	Rationale/Recommendation	
	Add new sentence after "enforceable.”: "They must also be concise so the policy is read from beginning to end and consequently encourages complete implementation and comprehension of the policy."	
	Disposition	
	The second draft of the NISTR document has been revised to address the comment.	

Comment Number: 096	Submitted by: DOS- Vickie L. McCray	Comment Type: __ Technical _X_ Editorial __ General
Reference: page c-3 Sect 2.2.5	Comment	
	The sentence after "Description" is incomplete.	
	Rationale/Recommendation	
	Finish that sentence or delete it.	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 097	Submitted by: DOS- Vickie L. McCray	Comment Type: _X_ Technical __ Editorial __ General
Reference: Bottom page c-3	Comment	
	Sect C.2.2.5 Examples: add one more example.	
	Rationale/Recommendation	
	Add: "Security organization not having a sign-off approval in the CM Process." to Sect C.2.2.5 Examples.	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 098	Submitted by: DOS- Vickie L. McCray	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page C-4, C.2.3.1.	Comment	
	Inadequate Periodic Security Audits. To "Description" paragraph add 1 more sentence.	
	Rationale/Recommendation	
	Add at very end of para, "Audits should not completely rely on interviews with the systems administrators."	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 099	Submitted by: DOS- Vickie L. McCray	Comment Type: __ Technical __ Editorial _X_ General
Reference: Page F-1	Comment	
	GAPP does not stand for "Generally Accepted Principles".	
	Rationale/Recommendation	
	Find the correct fill-in word for the 1st "P" or delete GAPP from Appendix F.	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 100	Submitted by: DOS- Vickie L. McCray	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page F-2	Comment	
	SCATA acronym is misapplied. SCATA most commonly is the acronym for Society for Computing and Technology in Anesthesia.	
	Rationale/Recommendation	
	Correct term is "SCADA	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 101	Submitted by: Aclara	Comment Type: __ Technical __ Editorial _X_ General

Reference: Pages 8-10, Sections 1.1, 1.2, 1.3

Comment

The opening statements of e NIST IR 7628 identify correctly that there has been a significant shift in the electric infrastructure of this country, from a one-way energy distribution system into a two-way flow of electricity and information. It is important to recognize that the electricity transmission and distribution network was designed by control systems engineers, not telecommunication experts or information technologists. Some of the critical control and management of this infrastructure may require us to consider carefully the implications of imposing specific technologies or protocols to the communications network. Adding security as an "after-thought" is unreliable.

For example, it is a common suggestion in many of the “Smart Grid Interoperability” initiatives that all communications between devices should use IP protocol. While it is well understood that a “standards based approach” for Smart Grid is a requirement, we may find that the specific standards chosen may need to address the specific needs of the system they are being applied to. For example, while we may believe that using IP protocol is, in general, a good idea for most of the Smart Grid, we may find specific instances where some inherent requirements of a given control system cannot be met with IP protocol, thus another standard which does meet these requirements must be chosen. It is our recommendation that NIST acknowledge within the opening paragraphs of this report that standards and protocols need to be applied with care in order to properly address the needs of Smart Grid.

It is also noteworthy that existing standards which are well suited for Smart Grid infrastructure may already exist, and conversely that adoption of “new technologies” and “new standards” carries some inherent risk. As an example, take APCO Project 25 (also known as TIA/ANSI P25). Project 25 a well established standard designed for high reliability wireless voice and IP protocol for use in public safety systems. P25 is supported by industry, government agencies, and public safety commissions alike. The Department of Homeland Security’s National Communication System (NCS), the Department of Defense, the National Association of State Telecommunications Directors (NASTD) and the National Telecommunications and Information Administration (NTIS) all recognize P25 as the standard for public safety. However, the use of P25 is not limited to public safety, and the interoperability of this system has been recognized as an advantage for use world-wide in many systems as a high-quality of service secure digital radio system, such as in railroad communications and in fleet management. Respectfully, it is suggested that NIST refrain from embracing or recommending only technologies which are being developed specifically for Smart Grid.

Rationale/Recommendation

Security of critical systems must be designed in to prevent flaws in the underlying architecture from creating exploitable weaknesses. The greatest weaknesses (as noted in 1.3) will be due to complexity and operator error, breaches at the interface between secured systems, socially engineered attacks, and cyber-attacks which exploit either weaknesses in the security system or architectural attacks due to the increased complexity and interconnectedness of the system.

Standards which are recommended today may become obsolete in the future. The guidelines set forth by NIST

Comment Number: 101	Submitted by: Aclara	Comment Type: __ Technical __ Editorial _X_ General

	should recognize that technologies change and that attacks on the Smart Grid aren't simply theoretical, they are in fact inevitable. A primary role of the NIST guidelines is to establish best practices for the Smart Grid; clearly it is a best practice to allow security on Smart Grid to follow a "continuous improvement process" in order to develop better strategies for new technology adaptation, system management, security, authentication, risk management and attack containment. NIST should encourage industry and potentially suggest that industry have economic incentives to continue to develop more robust solutions for Smart Grid, as this will drive innovation proactively rather than reactively. In order for the NIST recommendations to have the greatest value to Smart Grid, it is important that technology adopters understand not simply the guidelines but the reasons why they have been established. Otherwise, the Smart Grid industry will fall into the "check the box" mentality of security. The Smart Grid will by definition require education and training of those who operate it and quick yet well informed response to threats for those who maintain it.
	Disposition
	IP for the Smart Grid is being addressed by PAP 1 under the SGIP.

Comment Number: 102	Submitted by: Aclara	Comment Type: _X_ Technical __ Editorial __ General

Reference: Pages 15-17, Sections 2.1, 2.2, 2.3	Comment
	NIST has identified privacy on the Smart Grid as an area of significant concern, and that we need to develop appropriate protections for "personally identifiable information" (PII) collected and/or used within the Smart Grid. A question arises here about data exchanges between industrial or consumer nodes and head end systems. If the data exchange is with a logical node which contains a device specific identifier but does not tie that node to a specific premise, and the data itself does not identify the premise, is there a privacy concern? For example, if an operator located at a console connected to the head end system wishes to collect an ad-hoc electric meter reading from a house located at 1234 Main Street, the operator issues a query through the console, a database lookup determines that the device at that premise has a current IP address 192.168.144.120, and an IP request is sent to 192.168.144.120 requesting an ad-hoc reading. The premise device now responds and a packet is sent from 192.168.144.120 with the meter reading, which is then received and translated by the network head-end system to become a data element tied to that premise. The information is then displayed at the console where the request was issued from. In this example, is there a need for either (a) privacy of the request, (b) privacy of the response, (c) privacy of both the request and response or (d) this does not fall under the category of PII, thus there is no privacy risk.

Comment Number: 102	Submitted by: Aclara	Comment Type: _X_ Technical __ Editorial __ General
	Rationale/Recommendation	
	None	
	Disposition	
	Due to various discussions on the definition of personally identifiable information (PII), the NIST document has moved away from that term and is using the term personal information. The second draft of the NISTIR examines privacy issues with aggregated data, separation of duties and includes suggested privacy best practices with examples relevant to the Smart Grid.	

Comment Number: 103	Submitted by: Aclara	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 19, Sections 2.5.3, 2.5.4, 2.5.5	Comment	
	Regarding choice and consent to use PII, we need a better definition of PII. If a utility wishes to share demographics on usage patterns, say for example, system wide, and provides aggregate data without individual account numbers, is this PII? What if they release information by feeder, by substation, by street or even by transformer? By device IP address without releasing the information which ties the IP address to a residence? At what point does the data become PII, if any? Nelson television polling has been in use for many years and collecting just such information. As well, Yahoo and Google and many other internet search engines collect data “on the fly” in their search engines and other web pages, primarily for use in determining advertising to present to the user, but as well for long term demographic and statistical information to be later used for both research and target marketing. It is by no accident that this is commonplace and widely accepted as “the norm.” In these systems, “choice” is not an option. Use of the system automatically implies that your usage patterns are going to be collected and analyzed. There is in fact great value in collecting, analyzing, and disseminating the results of these usage patterns. Ultimately the average consumer of energy is not individually likely to make the best choices when it comes to patterns of usage (and behavior). Through analysis and simply because “the experiment” is being repeated millions of times, the “best practices” for reduction of energy use and cost will be empirically determined. With the data collected from Smart Grid, utilities and/or third party analysts will be enabled to provide “energy management services” for a fee, creating an entirely new service-sector industry which will earn revenues by assisting the average consumer in making wise choices. This is the same revenue model that CPA’s and tax preparation businesses have applied for decades: earn money by saving other people money.	
	Rationale/Recommendation	

<table>
<tr><td>Comment Number: 103</td><td>Submitted by: Aclara</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="3"></td><td colspan="2">None</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">Due to various discussions on the definition of personally identifiable information (PII), the NIST document has moved away from that term and is using the term personal information. A definition is included in the second draft of the NISTIR.</td></tr>
</table>

<table>
<tr><td>Comment Number: 104</td><td>Submitted by: Aclara</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference: Page 25, Section 3.3, Category 1</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">An attack identified at the CyLab which is part of the SEI at CMU theorized that there exists the ability to destabilize the Smart Grid control system without a direct attack on the payload of the messages sent to or from devices within the system, by simply loading and unloading the data channels which are in use between the communicating devices. This changes the timing of information being used for control, and can cause significant problems if it is not identified as a present risk. It does not attack the Confidentiality, Integrity, or Availability of the data – simply the timing of the data transfers. This is a very low tech but high risk form of attack.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">None</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">This is an interesting point and the vulnerability and bottom-up group will be reviewing this.</td></tr>
</table>

<table>
<tr><td>Comment Number: 105</td><td>Submitted by: Aclara</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="4">Reference: Page 71, Section DHS-2.8.15 / NIST SP 800-53 SC-17</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">Authentication by certificate must also provide for de-authentication in the case that the system identifies the possibility of an attack. In these instances, the system must “fail safe” to a mode where the damage risk of such an attack is minimized. Certificates must expire, but also must be able to be invalidated quickly and system wide.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">None</td></tr>
</table>

Comment Number: 105	Submitted by: Aclara	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 106	Submitted by: Aclara	Comment Type: _X_ Technical __ Editorial __ General
Reference: Pages 217, 219-220, Sections D.17 and D.24	Comment	
	NIST is correct in their assessment of the importance of key management. The use of a "pre-shared key" or "master root key" represents an inherent security risk. Some AMI vendors have chosen to use "pre-installed" individually unique keys as "master keys" for endpoints. This also represents a security risk, in several ways. First, it introduces a risk of key pollution or key manipulation at the manufacturing facility. Second, there is a risk of the key list being discovered, copied, or breached after manufacturing. In either case, management of a key installation process is difficult within the US borders, and even more so using off-shore manufacturing facilities. From a cryptographic standpoint, reducing the "brute force search space" to a list of keys in a database or on a CDROM is effectively turning what would be an intractable problem into a very simple one. Third, if a key can be installed with physical access to the device, there is a risk that the key will be manipulated after manufacturing. Finally, with a "pre-shared secret" approach, once a master key has been breached, there is no secure recovery mechanism, and if this is achieved in a large population of endpoints, the entire system integrity is at risk. NIST is also correct in their assessment that standard PKI appears to be inadequate for Smart Grid, and that many Smart-Grid devices have long operational lifetimes and thus special care must be given to protect these systems. Many devices which are deployed will not have any connectivity to appropriate trust centers.	
	Rationale/Recommendation	
	New cryptographic primitives and methods are needed which will address these security issues without introducing additional risks to Smart Grid. It should be recognized that the establishment of trust may take some time and may require significant computing capability at each endpoint, yet these systems must also allow for the quick revocation of trust and a "revert back to fail safe" if a breach or attack is detected. Last, there must be a fool-proof recovery mechanism which will properly reestablish cryptographic security after such potential threat, and this mechanism must be operable without connectivity to trust centers and it must not require every end device be physically reconfigured (visiting every meter in a system to inject new keys is not acceptable).	

Comment Number: 106	Submitted by: Aclara	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	Cryptography and key management are important areas for the Smart Grid. They will be examined more fully in the next version of the NISTIR.	

Comment Number: 107	Submitted by: Mark Freund Information Security Pacific Gas & Electric Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.7.2 Supplemental Guidance	Comment	
	The text in question reads: "The HAN is not controlled or owned by the utility, and should be treated as a hostile network by the AMI meter. Because of this, we recommend that AMI components should not request or accept information from HAN components. We recommend that AMI components should only push traffic to the home area network." It would be better to specify a higher level of trust for selected devices on the HAN where additional authentication, authorization and encryption takes place.	
	Rationale/Recommendation	
	Rather than ask for one way communication to HAN devices, provide a recommendation to provide for a higher level of trust with selected HAN devices. This would enable deployment of Demand Response on trusted HAN devices and provide a feedback mechanism. Note that the AMI network can verify compliance via the meter so the trusted HAN device can be verified in terms of compliance.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 108	Submitted by: University of Cambridge- Ross Anderson	Comment Type: _X_ Technical __ Editorial __ General
Reference: p. 67, 69, 101. 110	Comment	
	In our view there are two further pieces of work that will be vital to the success of this project, and in which the	

Comment Number: 108	Submitted by: University of Cambridge- Ross Anderson	Comment Type: _X_ Technical __ Editorial __ General

security research community could be engaged, as they are of technical interest as well as being important.

The first is to tie down a security policy for the core of the network. By a security policy, we mean a succinct statement of the protection goals, usually in the form of information flow constraints. The draft NIST IR 7628 hints at several such policies including multilevel confientiality (p 77 of the pdf pagination) and dual control (p 106) but implies that security requirements are still to be specified (p 11).

We believe the appropriate security policy at the core of the network is multilevel integrity, also known as the Biba model. Just as typical government systems allow information to flow upwards only from Unclassified to Confidential to Secret to Top Secret, and with various compartments at Secret and Top Secret, so control systems also have multiple levels. However, in their case the information flows downwards only, from the safety system (the level of highest assurance) to the control system, to the monitoring system, to the enterprise system and finally to the outside world. There is also some compartmentation at the control level (e.g. separate LANs for different parts of a large site) and even more compartmentation at the safety level (where systems often protect a specific machine or other resource).

This should interest the research community because it will be the first really large system with a multilevel integrity requirement, and because there are interesting second-order effects to explore. For example, just as in multilevel confidentiality systems one has to worry about covert channels (as in p 65 of your draft), so in control systems a service-denial attacks on the monitoring system may render a system unsafe. For example, it has happened that a worm infection of a server floods a SCADA network, depriving plant operators of visibility and leading to a precautionary shutdown, even though the control system and the primary safety systems were untouched. Such effects are novel, and important. Availability and integrity have received less attention from researchers than confidentiality so their interactions in control systems appear to be a fertile area for research.

Rationale/Recommendation

None

Disposition

An R&D sub group was recently established under the SGIP-CSWG. This comment has been forwarded to that group for evaluation and potential inclusion in the next version of the NISTIR.

Comment Number: 109	Submitted by: University of Cambridge- Ross Anderson	Comment Type: _X_ Technical __ Editorial __ General

Reference: p. 67, 69, 101.

Comment

The second area of urgent work is in the information flow policies required at the periphery – between the meter and the home area network. Here the NIST draft is undecided. At p 67 we find that AMI components should not

Comment Number: 109	Submitted by: University of Cambridge- Ross Anderson	Comment Type: _X_ Technical __ Editorial __ General

request or accept information from HAN components, while at p 69 we read that there must be a trusted path to users and at p 101 we find that information can indeed be passed from the HAN to the utility – just no control signals.

NIST should draw a clear distinction between two quite different meter architectures, both of which can be found in practice. In the first (which I might call 'thin' meters), the meter accepts from the utility the following day's prices, plus a small number of control signals such as 'please save energy now'. It sends back to the utility a reading of the energy used during the relevant charging periods the previous day. The communications between meter and utility thus amount to a few hundred bytes a day in each direction. Home energy management is left to user systems, which may or may not involve third parties such as Microsoft or Google.

The second type of architecture might be called the 'thick' meter; this passes detailed information to and from home appliances. Such an architecture gives the utility closer control over energy consumption but carries at least three costs. The first, as recognised by the NIST draft, is the risk that attacks might originate from (perhaps infected) home systems. The second, which has been emphasised in the rejection of a smart metering bill by the Dutch courts and is also a concern in the USA, is user privacy. The third is a concern of the UK energy regulator, among others: that if the tools used by the customer to manage energy are only provided by the utility – so that the customer goes to her power company's website to manage her home energy consumption – this raises serious issues of customer lock-in. It may also create conflicts of interest that undermine policy goals of reducing energy consumption and/or meeting carbon targets, inter alia by eliminating what might otherwise be a vigorous free market in energy management systems. Thick meters may also generate large volumes of data (perhaps 1Mb/day per customer) and may therefore require quite different network infrastructure to support them. GPRS may not be sufficient, and the same may apply to mesh networks.

Rationale/Recommendation

We would encourage NIST to bear this distinction in mind when clarifying policy on information flows at the periphery. It should also recognise that for standards setting to be successful, the standards must also be usable outside the USA. Equipment suppliers are global, and while different regional and national markets may make different choices on the thin versus thick meter issue, security standards should at least support a high-quality implementation of thin metering where privacy laws, or competition laws, demand it.

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 110	Submitted by: University of Cambridge- Ross Anderson	Comment Type: _X_ Technical __ Editorial __ General

Reference: p. 110	Comment
	Finally, we would urge caution on pushing standards on implementation detail. For example, the draft has (p 110) “The organization shall develop policies that stipulate the complexity (min/max length, combination of lower/upper case, numerals, special characters, etc.) level of the password for each criticality level.” This can be more complex than one might expect. With safety systems, as with weapons systems, passwords may be unacceptable; it may be a requirement that anyone physically present in the control room be able to close down a process that exceeds parameters. It may be a mistake to specify such matters too closely at a first pass. For good reasons, control engineers take standards much more seriously than IT people do. The electricity industry is over a century old; asset owners have learned to be much more wary of vendor lock-in than typical IT users; assets are valuable, with generating plant costing perhaps nine or ten-figure sums; assets are expected to last for decades; and electrity can kill. For all these reasons the IT industry approach of ‘there are hundreds of standards, so choose a few you like and ignore the rest’ and ‘ship it Tuesday and get it right by version 3’ just don’t work. For this reason, NIST should be more cautious about imposing standards for control systems than for IT systems.
	Rationale/Recommendation
	None
	Disposition
	This section has been removed and is included as a reference to the UCAIug OpenSG AMI Security Profile. High-level requirements are defined at the logical interfaces based on categorizations defined by logical interface categories. Refer to chapter 2 in the second draft of the NISTIR.

Comment Number: 111	Submitted by: OWASP's- Colin Watson	Comment Type: __ Technical _X_ Editorial __ General

Reference: DHS-2.15.3.2	Comment
	Supplemental Guidance - "The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts."
	Rationale/Recommendation
	We recommend: This text is amended to mention that anonymous/guest accounts are not recommended whenever reasonably avoidable.
	Disposition

Comment Number: 111	Submitted by: OWASP's- Colin Watson	Comment Type: __ Technical _X_ Editorial __ General
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 112	Submitted by: OWASP's- Colin Watson	Comment Type: _x Technical __ Editorial __ General
Reference: DHS-2.15.20/ NIST SP 800-53 AC-7 Unsuccessful Login Attempts	Comment	
	Comments: In possibly publicly accessible systems, it may be difficult to identify a particular user and multiple invalid authentication attempts should be restricted by total errors, and by errors from host address ranges, as well as by user account.	
	Rationale/Recommendation	
	We recommend: In Supplemental Guidance add "Automatic lockouts by remote address range may also need to be considered where multiple accounts are targeted in a brute force attack on authentication mechanisms."	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 113	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial _ General
Reference: DHS-2.15.19/ NIST SP 800-53 AC-9 Previous Logon Notification	Comment	
	It is useful to see not only the previous successful logon, but all recent significant activity.	
	Rationale/Recommendation	
	We recommend: Add "The system notifies the user of all successful and unsuccessful logon attempts in the last week/month/quarter" and add "The system notifies the user of all critical changes (CRUD) undertaken, on the system or by other methods (e.g., automatic patching), in the last week/month/quarter"	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included	

Comment Number: 113	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial _ General
	in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 114	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.16.2/ NIST SP 800-53 AU-2, AU-13 Auditable Events	Comment	
	The OWASP Enterprise Security API (ESAPI) Toolkits help software developers guard against security-related design and implementation flaws. The exception classes (e.g., in the Java EE version) define the types of security-related errors that should be identified and logged for web applications. http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API	
	Rationale/Recommendation	
	For web applications, the exception classes defined in the current version of the OWASP ESAPI project should be used as a guide.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 115	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.16.3/ NIST SP 800-53 AU-3 Content of Audit Records	Comment	
	For web applications, additional information is available which assist with the creation of a full audit trail.	
	Rationale/Recommendation	
	In Supplemental Guidance add "The user agent, remote host and any x-forwarded-for values should also be recorded for web enabled systems. In higher risk systems or more critical functions (identified by type, location or subject) the request headers, response headers and response body could also be included.".	

Comment Number: 115	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

OWASP Enterprise Security API, The Open Web Application Security Project, http://www.owasp.org/index.php/ESAPI

OWASP ESAPI Java EE error exception classes, The Open web Application Security Project, http://owasp-esapi-java.googlecode.com/svn/trunk_doc/org/owasp/esapi/errors/package-summary.html

For web applications, the record content defined in the current version of the OWASP ESAPI project should be used as a guide i.e.

- provide a mechanism for setting the logging level threshold that is currently enabled. This usually works by logging all events at and above that severity level, and discarding all events below that level.
- This is usually done via configuration, but can also be made accessible programmatically.
- ensure that dangerous HTML characters are encoded before they are logged to defend against malicious injection into logs that might be viewed in an HTML based log viewer.
- encode any CRLF characters included in log data in order to prevent log injection attacks.
- avoid logging the user's session ID. Rather, they should log something equivalent like a generated logging session ID, or a hashed value of the session ID so they can track session specific events without risking the exposure of a live session's ID.
- record the following information with each event:
  - identity of the user that caused the event,
  - a description of the event (supplied by the caller),
  - whether the event succeeded or failed (indicated by the caller),
  - severity level of the event (indicated by the caller),
  - that this is a security relevant event (indicated by the caller),
  - hostname or IP where the event occurred (and ideally the user's source IP as well),
  - a time stamp
- filter out any sensitive data specific to the current application or organization.

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 116	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.10.3/ NIST SP 800-53 CA-2 System Monitoring and Evaluation	Comment
	Penetration testing is an essential component of a comprehensive security program and is a key way in which compliance efforts related to FIPS 200 and NIST 800-53 can make a material impact on system security.
	Rationale/Recommendation
	Also in the supplemental guidance, "Changing security requirements and discovery of vulnerabilities necessitate a review.", changes to the environment such as new threats should also necessitate a review.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 117	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.8.7/ NIST SP 800-53 SC-2, SC-7, SC-32 Boundary Protection	Comment
	Administrative functions should be appropriately segregated from user activity, so the latter cannot access or utilize administrator functionality.
	Rationale/Recommendation
	We recommend adding to the Supplemental Guidance, "Web administrative interfaces should use separate authentication methods for users of any other resources. This may include isolating the administrative interface on a different domain and with additional access controls. In a web application environment, if a higher value system does not use strong authentication and encrypted channels to log on to the interface, the system may be vulnerable from privilege escalation, eavesdropping, man in the middle and replay attacks." Administrative Interfaces, pp220-222, A Guide to Building Secure Web Applications and Web Services, v2.0, The Open Web Application Security Project, http://www.owasp.org/index.php/Category:OWASP_Guide_Project
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in

Comment Number: 117	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
	the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 118	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.16/ NIST SP 800-53 SC-18 Mobile Code	Comment	
	We recommend providing a greater level of detail and references to specific vulnerabilities - including XSS, CSRF and others. We also recommend referencing external best practices like the OWASP Top 10: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 119	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.17/ NIST SP 800-53 SC-19 Voice-Over Internet Protocol	Comment	
	If used, any administrative access points should be included in vulnerability assessment and penetration testing efforts.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document	

Comment Number: 119	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

	which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 120	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.14.3/ NIST SP 800-53 SI-3 Malicious Code Protection	Comment
	Malicious code may be present in custom-built software. This could include time bombs, back doors, Easter eggs, salami attacks and other types of attack that could affect business processes. Traditional anti-malware products are not built to detect such code, and instead secure development, procurement, configuration and monitoring practices are required to ensure software does not perform functions other than those intended. Malicious Code Verification Requirements, V13, OWASP Application Security Verification Standards (ASVS), The Open Web Application Security Project http://www.owasp.org/index.php/ASVS
	Rationale/Recommendation
	We recommend that enhancements item 12 "12. The authenticity of all firmware/software shall be verified prior to loading on any component of the AMI system or device connected to the AMI network." should also mention that verification needs to "examine and test all software for malicious code". Also add an enhancement "Verify software quality (including security) before configuration and monitors for, and performs audits to identify, unauthorized changes to production software code."
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 121	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.14.10/	Comment
	Software developers often expect a single value for each data input, but bad design or a malicious user might

<table>
<tr><td>Comment Number: 121</td><td>Submitted by: OWASP's- Colin Watson</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5">NIST SP 800-53 SI-10 Information Input Accuracy, Completeness, Validity, and Authenticity</td><td colspan="2">lead to more than one value being submitted.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">The format and content of structured data should be tested against what is defined. Information could be accurate, complete, valid and authentic but still be contrary to valid business logic. These concerns need to be built into the checking processes.Validity checks should include "character set, length, numerical range, acceptable values, integrity, character set and cardinality".
Also where a specification exists for data (e.g., an XML schema, data interchange standard), both compliance with the permissible structure and the values contained should be undertaken. The validity of information may depend on other factors such as business logic, timing and related transactions.
Reference: Data Validation, pp161-172, A Guide to Building Secure Web Applications and Web Services, v2.0, The Open Web Application Security Project, http://www.owasp.org/index.php/Category:OWASP_Guide_Project</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.</td></tr>
</table>

<table>
<tr><td>Comment Number: 122</td><td>Submitted by: OWASP's- Colin Watson</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference: DHS-2.14.12/ NIST SP 800-53 SI-12 Information Output Handling and Retention</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">There should be appropriate encoding/encryption of information generated by the system or supplied to other systems. The proper validation, formatting and encoding of such information is just as important as making sure the inputs are correct. Incorrect output checking could leak sensitive information. For web applications, incorrect output encoding can lead to issues such as cross-site scripting (XSS) attacks on web browser users.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">None</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document</td></tr>
</table>

Comment Number: 122	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
	which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 123	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix C NIST CSCTG Vulnerability Classes	Comment	
	In C.3.1.3. Authorization Vulnerability, add "Insecure direct object references" and "Failure to restrict URL access" to examples.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 124	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix C NIST CSCTG Vulnerability Classes	Comment	
	In C.3.1.7. General Logic Errors, add "Business logic flaw" to examples.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has been revised to address the comment.	

Comment Number: 125	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix C NIST CSCTG Vulnerability	Comment	
	In C.3.1.8. Input Validation, change title to "Input and Output Validation", and add "Unvalidated redirects and forwards" to examples.	
	Rationale/Recommendation	

Comment Number: 125	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Classes	None	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 126	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix C NIST CSCTG Vulnerability Classes	Comment	
	In C.3.1.12. Protocol Errors, add "Insufficient transport layer protection", "Use of weak SSL/TLS protocols", "SSL/TLS key exchange without authentication", "SSL/TLS weak key exchange" and "Low SSL/TLS cipher strength" to examples.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 127	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix C NIST CSCTG Vulnerability Classes	Comment	
	In C.3.1.13. Range and Type Error Vulnerability, add "Cardinality incorrect", "Value integrity modification" and "Sequencing or timing error" to examples.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has been revised to address this comment.	

Comment Number: 128	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 128	Submitted by: OWASP's- Colin Watson	Comment Type: _X_ Technical __ Editorial __ General

Reference: Appendix C NIST CSCTG Vulnerability Classes	**Comment**
	In C.3.1.15. Session Management Vulnerability, add "Cross site request forgery", "Cookie attributes not set securely (e.g. domain, secure and HTTPonly)" and "Overly long session timeout" to examples.
	Rationale/Recommendation
	None
	Disposition
	The second draft of the NISTIR has been revised to address this comment.

Comment Number: 129	Submitted by: Information and Privacy Commissioner of Ontario, Canada & The Future of Privacy Forum- Ann Cavoukian	Comment Type: __ Technical __ Editorial _X_ General

Reference: Chapter 2	**Comment**
	We are pleased to see in the draft report that a high level Privacy Impact Assessment was completed. Too often it is assumed that security and privacy are one and the same, or that we must sacrifice privacy for the sake of security. The argument that we must sacrifice privacy for security, however, is erroneous. We believe that we can, and must, have both privacy and security, which may be achieved through Privacy by Design. Privacy by Design or PbD is a concept developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian in the '90s which ensures the protection of privacy by embedding it into the design specifications of information technology, accountable business practices, physical environments and networked infrastructure – making privacy the default. She has consistently advanced the view that it is not necessary to trade off privacy against equally important goals such as security, transparency or functionality. In our co-authored paper, which we are enclosing, we put forward the argument that while the Smart Grid is an excellent idea, the focus has been so singularly directed at controlling energy use and issues of security that privacy has not been given equal consideration. Given the amount of personal information that will be involved in an endeavour such as the Smart Grid, we strongly believe that we must give serious consideration to strong data management practices and privacy protection. Security or safeguarding of personal information is a fundamental principle within the concept of privacy as outlined in Chapter 2, where The Cyber Security Coordination Task Group used the Generally Accepted Privacy Principles (GAPP) as a privacy framework. President Barack Obama has stated, "America's economic prosperity in the 21st century will depend on

Comment Number: 129	Submitted by: Information and Privacy Commissioner of Ontario, Canada & The Future of Privacy Forum- Ann Cavoukian	Comment Type: __ Technical __ Editorial _X_ General
	cybersecurity.” The same statement is true for the protection of privacy and economic prosperity. Return on investment for the Smart Grid will be low if the grid only offers the same level of privacy protection as, for example, the Internet. As we know, the existing identity infrastructure of the Internet is no longer sustainable due to the high level of fraudulent activity online, which has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done at these early stages of the Smart Grid to ensure that consumer confidence and trust results in high uptake for essential components of the grid, such as enrolling in energy conservation programs (i.e. load management) and smart appliances. Consumer control of electricity consumption and control of one’s personal information must go hand in hand. Doing so will ensure that consumer confidence and trust is gained, and that participation in the Smart Grid contributes to the vision of creating a more efficient and environmentally friendly electrical grid, as well as one that is protective of privacy. This will result in a positive-sum (win-win) outcome, (not zero-sum), where both environmental efficiency and privacy may coexist.	
	Rationale/Recommendation	
	As the risk management framework for the Smart Grid continues to develop, designers of the Smart Grid and utility providers must ensure that unauthorized access to personal information traveling through the electrical grid is minimized, as much as possible. Special attention should be paid to insider threats within utilities and those organizations that provide services using consumers’ energy consumption information. The Institute for Information Infrastructure Protection (I3P) is conducting leading-edge research in this area. We are enclosing our paper, SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, which contains more information on these matters. We hope that this material may assist with your revision of the report, particularly in expanding the section of the report dealing with privacy. Thank you for the opportunity to comment. Please feel free to contact us for more information. We would be happy to collaborate on building privacy into the Smart Grid.	
	Disposition	
	These comments will be addressed in the next draft of the NISTIR.	

Comment Number: 130	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.2.2	Comment	
	The Rational for this requirement states the risk of gaining access to management services. As encryption	

Comment Number: 130	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Supplemental Guidance p. 57	certificates are noted as a method of access elsewhere in this document (see DHS-2.8.15), a suggestion that different certificates be used to prevent rights escalation helps clarify the purpose of this requirement.	
	Rationale/Recommendation	
	Update second sentence to include certificates: Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses, different encryption certificates, or protocol ports (e.g., TCP ports), combinations of these methods, or other methods as appropriate.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 131	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.13.1 Requirement p. 63	Comment	
	Collaborative computing capabilities can be very helpful for troubleshooting support and also mitigate unauthorized access (e.g. Substation access). If wholly hosted within the enterprise and if properly configured to ensure that control data is provided sufficient quality of service, additional threat vectors can be can be mitigated. Explicit indication of activation and the ability to disable the mechanisms is appropriate to reduce accidental disclosure, but should be balanced against the security benefits, especially in areas that are typically unattended.	
	Rationale/Recommendation	
	Recommend deletion of para. “Alternative statement” as the term "current state" for a technology can evolve. Suggest new wording for first paragraph: The use of collaborative computing mechanisms on AMI components can introduce additional threat vectors that must be mitigated. Explicit indication of use to the local users must be provided.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included	

Comment Number: 131	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

	in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 132	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.8.16.1 Requirement p. 64	Comment
	The last paragraph contains the statement "Given the current state…", indicating vulnerabilities at a point in time (in the past). If the vulnerabilities have been or will be addressed, the risk of mobile code is mitigated. The other content in this requirement addresses how an organization should address mobile code. Recommend deletion of this paragraph.
	Rationale/Recommendation
	Recommend deletion of the paragraph starting with "Given the current state…"
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 133	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.8.16.2 Supplemental Guidance - first paragraph p.64	Comment
	Clarification. While the term "development" can be consider the same as "modification", modification can occur without the use of development tools. (Development on the AMI system can be addressed by not allowing installation of development tools on the system)
	Rationale/Recommendation
	Recommend insertion of the word "modification" as shown: Procedures need to prevent the development, modification, acquisition, or introduction of unacceptable mobile code within the AMI system.
	Disposition

Comment Number: 133	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 134	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.16.2 Supplemental Guidance - second paragraph p.64	Comment	
	The rational for this requirement describes the process of performing firmware upgrades to meters. Firmware upgrades to meters are required to address new features and may be required to mitigate vulnerabilities. Digital signing of mobile code and other configuration management tools have been developed to address mobile code deployment. The first para. states a good process for the use of mobile code.	
	Rationale/Recommendation	
	Recommend deletion of second paragraph that starts with "Mobile code should not be used…"	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 135	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.17.1 Requirement p.65	Comment	
	The last sentence contains the statement "Given the current state…", indicating vulnerabilities at a point in time (in the past). If the vulnerabilities have been or will be addressed, the risk of VOIP techology is mitigated. The other content in this requirement addresses how an organization should address VOIP technology. Recommend deletion of this sentence.	
	Rationale/Recommendation	

Comment Number: 135	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

	Recommend deletion of the sentence: Given the current state of this technology and/or the ability to secure it would substantially increase the security risk at this time.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 136	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.8.17.2 Supplemental Guidance p. 65	Comment
	The last sentence contains the statement "Given the current state…", indicating vulnerabilities at a point in time (in the past). If the vulnerabilities have been or will be addressed, the risk of VOIP technology is mitigated. The other content in this requirement addresses how an organization should address VOIP technology. Recommend deletion of this sentence.
	Rationale/Recommendation
	Recommend deletion of the sentence: Given the current state of this technology and/or the ability to secure it would substantially increase the security risk at this time.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 137	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: __ Technical _X_ Editorial __ General

Reference: DHS-2.15.7.3 Requirement	Comment
	While an important requirement, the word "never" is difficult to verify as it addresses unforseen future changes.
	Rationale/Recommendation

Comment Number: 137	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: __ Technical _X_ Editorial __ General
Enhancements - #7 p. 99	Recommend change of "never allow" to "prevent"	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 138	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.15.27 Personally Owned Information p. 109	Comment	
	The numbered list in this requirement outlines actions of personally owned equipment, while the leading paragraph describes personally owned information. Recommend renaming of the requirement to address personal IT equipment	
	Rationale/Recommendation	
	Suggest replacement of the requirement as follows: Personally Owned IT Equipment	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 139	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.15.27.1 Requirement p. 109	Comment	
	The numbered list in this requirement outlines actions of personally owned equipment, while the leading paragraph describes personally owned information. Recommend rewording of first paragraph to match numbered list.	
	Rationale/Recommendation	
	Suggest replacement of the first sentence with the following: The organization must restrict the use of personally	

Comment Number: 139	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

	owned IT equipment from access to the AMI system or AMI system user workstations that are used for official organization business.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 140	Submitted by: Lockheed Martin- Robert Jepson	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.15.27.2 Supplemental Guidance p. 109	Comment
	The numbered list in this requirement outlines actions of personally owned equipment, while the leading paragraph describes personally owned information. Recommend rewording of this paragraph to match numbered list.
	Rationale/Recommendation
	Suggest replacement with the following: The organization must establish strict terms and conditions on the access of AMI components with personally owned equipment.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 141	Submitted by: American Systems- John (Jack) Emanuelson	Comment Type: _X_ Technical __ Editorial __ General

Reference: D.53 TRAFFIC ANALYSIS, Page D-16	Comment
	The opening sentence is misleading. Traffic analysis (TA) is not the exclusively the study of “encrypted” communications characteristics. This fact is indicated in the final sentence of the section, i.e., “. . . . . even if operational information were encrypted, TA could provide an attacker, etc.”
	Rationale/Recommendation

Comment Number: 141	Submitted by: American Systems- John (Jack) Emanuelson	Comment Type: _X_ Technical __ Editorial __ General
	SUGGEST that the first sentence be rewritten as follows: Traffic Analysis (TA) is the examination of patterns and other communications characteristics to glean information. Such examination is possible, even if the communication is encrypted.	
	Disposition	
	Addressed by incorporating suggested changes verbatim.	

Comment Number: 142	Submitted by: Don DiNaro	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	Will this be limited to electrical power generation, or will it allow Power companies & distributors to go into the Cable internet, HDTV and Telephone business also?	
	Rationale/Recommendation	
	None	
	Disposition	
	The NISTIR contains requirements for the power industry and does not address policy issues. Policy issues are outside the scope of the SGIP-CSWG.	

Comment Number: 143	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General
Reference: DHS-2.8.2.2	Comment	
	"different network addresses or protocol port (e.g., TCP ports)" That doesn't seem like much of a separation if they are both on the same host, but seem acceptable if they are on multiple hosts. For example if mail and web running on one server, compromise one and you can probably compromise the other.	
	Rationale/Recommendation	
	Perhaps a better or extra addition would be different user permissions on the system per application so if one is compromised (and it's not root/admin) it forces the attacker to also escalate privs. to (fully) compromise the other	

Comment Number: 143	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

	services on the box.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 144	Submitted by: Ercot- Michael Sconzo	Comment Type: __ Technical _X_ Editorial __ General

Reference: DHS-2.8.3.2	Comment
	#2 "Each AMI component...within the isolatio"
	Rationale/Recommendation
	Shouldn't that read "isolation"
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 145	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

Reference: DNS-2.8.8.3	Comment
	#3 "must not create a denial of service of rail to an unprotected open state" This seems to contradict (maybe in wording alone) the "availability" mentioned later in that paragraph. It seems if it doesn't fail in open state it would fail to a closed state and not work. However, I see the argument that it shouldn't be unprotected, perhaps there should be a note that the implementer should take into account the criticality of the system.
	Rationale/Recommendation

Comment Number: 145	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

	None
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 146	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

Reference: ASAP-2.8.24.3	Comment
	"ARP spoofing and similar attacks may allow an attack to subvert natural automated network behavior in order to all the attacker to get "in the middle" of valid communication"
	Rationale/Recommendation
	Change all to "allow". Although I don't think I'm entirely clear on "natural automated network behavior" means. Seems like a lot of words for the network structure, or something equally simplistic.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 147	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.12.11.1	Comment
	"review the data at a minimum monthly, if not daily or more frequently"
	Rationale/Recommendation
	Maybe remove the "daily" as it seems redundant.
	Disposition

Comment Number: 147	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 148	Submitted by: Ercot- Michael Sconzo	Comment Type: _X_ Technical __ Editorial __ General

Reference: DHS-2.14.6.2	Comment
	The first sentence is a killer and seems to do a lot of hand waving and not say much of anything with a lot of words. I'm not too sure what to offer as a suggestion, but it seems to say "It supports the functions that it does securely".
	Rationale/Recommendation
	So maybe it should say "The AMI management system should be designed with security in mind, such that AMI devices will require proper security to function"?
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 149	Submitted by: Open Secure Energy Control Systems, LLC- Stanley Klein	Comment Type: _X_ Technical __ Editorial __ General

Reference: ET	Comment
	The actor originally shown as SCADA/DMS and now shown as DMS should be restored to SCADA/DMS. I interpret the SCADA to be the balancing authority SCADA from which commands are sent to generators, not the distribution SCADA. The PEV is essentially another generator. The balancing authority has the choice of communicating directly or through an aggregator. The DMS probably needs to know what is going on, but not necessarily in the same way the balancing authority does.

Comment Number: 149	Submitted by: Open Secure Energy Control Systems, LLC- Stanley Klein	Comment Type: _X_ Technical __ Editorial __ General

	Rationale/Recommendation
	Issue: Suggest discussion on adding an aggregation characteristic to the interface descriptions. These would be paired interfaces that carry aggregated and disaggregated data that otherwise has the same requirements. The third party actor should be restored to the diagram with its interface to the home (which really generalizes and includes auto repair facilities). My original thought was that this is an entertainment interface, but the group realized that it is more likely a maintenance interface to the PEV and HAN functionality (e.g., patch maintenance of HAN and PEV s/w). The actor marked as metering should also include billing, back office, and inter-service-area transaction settlement functions. Note: I still have to go through the individual ET interfaces, and it is possible some new interface classes will result. I think ET will have interfaces that are real-time, high integrity, high confidentiality/privacy, bandwidth-limited between SCADA or aggregator and the PEVs. The interfaces will require high availability in the aggregate (not to any one PEV but sufficient to control enough PEVs to maintain grid balance).
	Disposition
	The diagrams have all been revised and there is an overall functional logical architecture in the second draft of the NISTIR.

Comment Number: 150	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: __ Technical __ Editorial _X_ General

Reference: Overall	Comment
	Network clouds potentially confuse the audience while adding little value. If we define interfaces correctly throughout, then definition of networks should be unnecessary. A concern exists that the network clouds could seem to be prescriptive.
	Rationale/Recommendation
	Recommend deletion
	Disposition
	Updated architecture diagrams have removed the use of network clouds.

Comment Number: 151	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	Some actors on diagrams do not seem to look consistent with the definition of an actor: i.e. Distribution Operator (DGM) should it be included with DMS functions?; Customer (AMI);	
	Rationale/Recommendation	
	None	
	Disposition	
	The diagrams have all been revised and there is an overall functional logical architecture in the second draft of the NISTIR.	

Comment Number: 152	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Some acronyms not spelled out: i.e. 'DA Field Devices' (AMI), MDMS (AMI), ESI Network (AMI), DER & PEV (DGM), MDMS (DR), DMS (ET),	
	Rationale/Recommendation	
	None	
	Disposition	
	A strong effort is made to spell out each acronym upon first use in the document. Acronyms are defined in Appendix F – Glossary and Acronyms.	

Comment Number: 153	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Terms to describe actors in market domain should be consistent.	
	Rationale/Recommendation	
	Recommend using terms defined in NAESB standards	
	Disposition	

Comment Number: 153	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
	The diagrams have all been revised and there is an overall functional logical architecture in the second draft of the NISTIR.	

Comment Number: 154	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	Lack of consistency on which domains various actors fall into (i.e. ITO/RTO)	
	Rationale/Recommendation	
	None	
	Disposition	
	The diagrams have all been revised and there is an overall functional logical architecture in the second draft of the NISTIR.	

Comment Number: 155	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Interface AMI 22 displays arrow from Billing to itself (Billing), this does not make sense.	
	Rationale/Recommendation	
	None	
	Disposition	
	AMI Interfaces have been updated. The billing pointing to itself has been removed.	

Comment Number: 156	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 18	Comment	
	Page 18 • Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are	

Comment Number: 156	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

feasible.

- Intelligent Electronic Devices (IEDs) can be limited in compute power, but that is becoming less of an issue as newer more capable devices become available. However, the large legacy of devices in the field will need be addressed through mitigating technologies and methods.
- Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls (either physical or cryptographic) appropriate for wireless
- None of the communication protocols currently used (primarily Distributed Network Protocol (DNP3) and sometimes International Electrotechnical Commission (IEC) 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear.
- Some of the equipment is legacy (particularly the Remote Terminal Units (RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment
- Key management with thousands of devices is an issue that needs to be solved in terms of operational feasibility and cost.
- Many of the SCADA Masters may have no way to add security without complete replacement
- Many devices have no notion of a user or a role making security management a challenge.
- Often no security event information available from these systems
- No standard for security events or logging

Rationale/Recommendation

Recommend moving the following bullets from “Constraints” to “Issues”:

Disposition

In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Page 20

- Different organizations can have different security policies, different enforcement levels, and different security technologies, thus possibly leading to interoperability issues, security gaps, and decreased availability of data.
- The most commonly used protocol, IEC 60870-6 (ICCP), has authentication and encryption security through IEC 62351, but this security is not widely implemented.

Comment Number: 157	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 157	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 20	Comment	
	Page 20 • Different organizations can have different security policies, different enforcement levels, and different security technologies, thus possibly leading to interoperability issues, security gaps, and decreased availability of data. • The most commonly used protocol, IEC 60870-6 (ICCP), has authentication and encryption security through IEC 62351, but this security is not widely implemented.	
	Rationale/Recommendation	
	Recommend moving the following bullets from “Constraints” to “Issues”:	
	Disposition	
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.	

Comment Number: 158	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 22	Comment	
	Page 22 • Privacy can be a major issue related to sensitive customer information • Privacy of the customer information may become an issue if sensitive data is provided to the GIS • Privacy of customer information within the CIS as well as collected through the AMI headend will be critical	
	Rationale/Recommendation	
	Recommend moving the following bullets from “Constraints” to “Issues”:	
	Disposition	
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.	

Comment Number: 159	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 159	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Page 23	Page 23 • Privacy can be a major issue related to sensitive customer information • Privacy of the customer information may become an issue if sensitive data is provided to the GIS • Privacy of customer information within the CIS as well as collected through the AMI head-end will be critical
	Rationale/Recommendation
	Recommend moving the following bullets from “Constraints” to “Issues”:
	Disposition
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 160	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 24	Comment
	Page 24 • Load management signals, whether direct load control, indirect pricing, or energy request signals, can have profound effects on customer reactions. If these signals are compromised, serious power system consequences could result, as well as serious customer reactions to the Smart Grid. • Both the AMI network and the public Internet pose privacy and other security issues. The AMI network may have limited bandwidth for some types of information exchanges.
	Rationale/Recommendation
	Recommend moving the following bullets from “Constraints” to “Issues”:
	Disposition
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 161	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 25	Comment
	Page 25 Category 7

Comment Number: 161	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
	• The information exchange requirements between the DMS and the AMI head-end, except for outage information, are not known. Category 8 • IED's and embedded sensors have limited computing power to authenticate each other • Rogue nodes can be added by attackers. This rogue nodes might have much more computing power than the real nodes • Media is usually narrowband, limiting the volume of traffic and impacting the types of security measures and protections that are feasible.	
	Rationale/Recommendation	
	Recommend moving the following bullets from "Constraints" to "Issues":	
	Disposition	
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.	

Comment Number: 162	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 26	Comment	
	Page 26 • Wireless media is often less expensive than wired media, which means that wireless vulnerabilities exists, and will require security controls (either physical or cryptographic) appropriate for the wireless network. • None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear. • Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment	
	Rationale/Recommendation	
	Recommend moving the following bullets from "Constraints" to "Issues":	
	Disposition	
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.	

Comment Number: 163	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 27

Comment

Page 27

- Communications media is usually narrowband, limiting the volume of traffic and impacting the types of security measures that are feasible for cyber protection and monitoring.
- IEDs can be limited in compute power, but that is becoming less of an issue as newer more capable devices become available. However, the large legacy of devices in the field will need be addressed through mitigating technologies and methods.
- None of the communication protocols currently used (primarily DNP3 and sometimes IEC 61850) are typically implemented with security measures, although IEC 62351 (which are the security standards for these protocols) is now available but implementation adoption and feasibility is not yet clear. Some of the equipment is legacy (particularly the RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment

Rationale/Recommendation

Recommend moving the following bullets from “Constraints” to “Issues”:

Disposition

In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 164	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 28

Comment

Page 28

- Microprocessor constraints on memory and compute capabilities
- Legacy end-devices and systems
- Legacy communication protocols

Rationale/Recommendation

Recommend moving the following bullets from “Constraints” to “Issues”:

Disposition

In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 165	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 29	Comment
	Page 29 • Microprocessor constraints on memory and compute capabilities • Legacy end-devices and systems • Legacy communication protocols
	Rationale/Recommendation
	Recommend moving the following bullets from “Constraints” to “Issues”:
	Disposition
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 166	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 24	Comment
	A number of bullets in the ‘Constraints section’ describe proposed controls, which are not constraints Page 24 • These systems are usually organized into different security domains, so pertinent system separation measures must be taken (such as separate IP networks, a well configured firewall, etc.)
	Rationale/Recommendation
	None
	Disposition
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 167	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 26	Comment
	A number of bullets in the ‘Constraints section’ describe proposed controls, which are not constraints Page 26

Comment Number: 167	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

	• Since confidentiality has not been perceived as important, and where the media and compute constraints apply, payload encryption may not necessarily be required for general messaging
	Rationale/Recommendation
	None
	Disposition
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 168	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Page 27	Comment
	A number of bullets in the 'Constraints section' describe proposed controls, which are not constraints Page 27 • Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls (physical or cryptographic) appropriate for wireless
	Rationale/Recommendation
	None
	Disposition
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.

Comment Number: 169	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General

Reference: Diagrams	Comment
	Accounting Issues: WAS diagram has 29 interfaces, Category-Logical Interfaces table has only 27 interfaces:
	Rationale/Recommendation
	None
	Disposition
	In the second draft of the NISTIR the architecture diagrams have been updated.

Comment Number: 170	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Diagrams	Comment	
	Accounting Issues: DGM diagram has 35 interfaces, Category-Logical Interfaces table has 36 interfaces:	
	Rationale/Recommendation	
	None	
	Disposition	
	In the second draft of the NISTIR the architecture diagrams have been updated.	

Comment Number: 171	Submitted by: DHS NPPD NCSD CSSP- Tom Dion	Comment Type: _X_ Technical __ Editorial __ General
Reference: Diagrams	Comment	
	Accounting Issues: AMI diagram has 42 interfaces, Category-Logical Interfaces table has only 41 interfaces:	
	Rationale/Recommendation	
	None	
	Disposition	
	In the second draft of the NISTIR the architecture diagrams have been updated.	

Comment Number: 172	Submitted by: Honeywell- Tom Markham	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 2	Comment	
	NISTIR 7628 correctly states that most PUCs and utilities do not have mature privacy policies. Subsection 2.3 (page 9) lays out the high level principles for privacy but states These principles can be used by authorities and organizations as a starting point for the development of appropriate protections for PII collected and/or used within the Smart Grid. Honeywell strongly believes that protection of consumer privacy is critical to the adoption of Smart Grid, including	

Comment Number: 172	Submitted by: Honeywell- Tom Markham	Comment Type: _X_ Technical __ Editorial __ General

	devices communicating on the Home Area Network (HAN). If home owners even fear their privacy will be compromised by participating in the Smart Grid it could create a backlash which stalls adoption of energy saving technologies. One can imagine communicating appliances reporting their brand, model and date of manufacture to the utility which then sells the data to home appliance service organizations (e.g. Minnegasco or Centerpoint Home Service Plus) and local appliance stores. Even if the devices do not report this information explicitly, it may be possible to derive this information based upon the Media Access Control (MAC) address or serial number associated with a piece of equipment. The MAC address is unique to each piece of equipment and is routinely used today to determine the equipment manufacturer. Releasing information on the types of appliances in a home, their age and usage patterns is a violation of privacy and could subject home owners to unwanted telemarketers and junk mail. Organizational firewalls should be required within the utilities such that the data collected from home owners is only used for the authorized purposes. The data MAY be used for load forecasting and potential efficiency analysis in the aggregate (e.g., 30% of homes within the utility service area have refrigerators older than 12 years old). The data MAY NOT be used to identify an individual home for purposes other than those specifically allowed by law or homeowner consent.
	Rationale/Recommendation
	NISTIR must include clear, strong language spelling out specific privacy protection. This Honeywell position is consistent with the Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information http://www.naruc.org/Resolutions/privacy_principles.pdf
	Disposition
	The privacy chapter of the second draft of the NISTIR has been revised and now includes suggested privacy practices relevant to the Smart Grid.

Comment Number: 173	Submitted by: Honeywell- Tom Markham	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 3,	Comment
	Categories 10, 11, and 12 they have Confidentiality at a L-M.

Comment Number: 173	Submitted by: Honeywell- Tom Markham	Comment Type: _X_ Technical __ Editorial __ General
Page 28	Rationale/Recommendation	
	These should be listed as M. This data can not only be used to determine when a home owner is away (promoting burglary), but can also disclose information regarding a processing plant which not only gives their competitors information but provides reconnaissance information for a cyber attack.	
	Disposition	
	Technical discussions are still ongoing for the confidentiality levels of logical interface categories.	

Comment Number: 174	Submitted by: Honeywell- Tom Markham	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 3, Page 30	Comment	
	Category 13 (page 30) It should be noted that availability may also be related to the safety of field crews. If a field crew is unable to communicate with a substation, it could lead to a hazardous situation. Alternately, if the crew does not work until the communications with the substation is confirmed, then jamming this signal could prolong outages.	
	Rationale/Recommendation	
	None	
	Disposition	
	Logical interface categories and definitions have been revised in the second draft of the NISTIR.	

Comment Number: 175	Submitted by: Honeywell- Tom Markham	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 – AMI Security requirements (P61), DHS-2.8.8.3	Comment	
	Part 3 of this requirement seems to contradict itself. What are the options if a cryptographic mechanism (e.g. hardware encryption device) fails? • The system could bypass the failed encryption device and send the data in the clear. • This constitutes failure to an unprotected open state. • The system could not send traffic because the means of encrypting it is no longer available. Not being able to communicate is in itself a denial of service.	

<table>
<tr><td colspan="2">Comment Number: 175</td><td>Submitted by: Honeywell- Tom Markham</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5"></td><td colspan="3">Consider the scenario in which a thief attempts to steal power by tampering with the cryptographic component of a smart meter. (E.g. charging a PEV without paying for it) The requirement as currently written states that “Failure of a cryptographic mechanism must not create a denial of service.” Obviously the intent is not to require the utility to deliver free power to those who induce a failure in a cryptographic component.
Is the intent of this requirement to say – Failure of a cryptographic mechanism or associated key management shall lead to graceful degradation. The failure shall not lead to a cascading impact on the larger power grid. To the extent practical, the system should attempt to deliver power as it did prior to the failure.
This comment also applies to DHS-2.15.14.3 Requirement Enhancements on page 102.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 176</td><td>Submitted by: Back Bone Security- Jim Wingate</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="4">Reference: Overall</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Based on a very cursory scan, it didn’t appear there was much at all in the way of addressing the vulnerability from the insider threat.
The insider threat must be explicitly addressed. The word “insiders” is used one time in the 236 page document. A trusted insider with detailed knowledge about the currently installed host and network security systems can easily plan their activities to subvert even the most technically sophisticated protection mechanisms.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">To prevent a cascading catastrophe across the grid, it may be necessary to compartmentalize the grid network architecture in such a way that it would be extraordinarily difficult for a lone trusted insider gone bad to cause significant damage or widespread outage. Perhaps it might even require implementation of 2-person control at some level(s) within the network much like the 2-person concept used in nuclear command and control.</td></tr>
</table>

Comment Number: 176	Submitted by: Back Bone Security- Jim Wingate	Comment Type: _X_ Technical __ Editorial __ General

	Disposition
	The security requirements are intended to address threats from insiders and external entities. For the next version of the NISTIR, we will do additional analysis to ensure we address the insider threat.

Comment Number: 177	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 1.4 Page 4	Comment
	Reference: “The requirements will not be allocated to specific systems, components, or functions of the Smart Grid.” This is so broad as to dilute the utility of such requirements, since "the Smart Grid as a whole" is an extremely large, complex and varied domain with many disparate systems and devices. It would be like the Federal Government specifying security requirements for the entirity of government without allocation to specific systems, components or functions. For example, the security requirements of a nuclear submarine base are rather different from that of the local Navy recruiter's office even though both are in the same branch of the military.
	Rationale/Recommendation
	None
	Disposition
	The second version of the NISTIR has been revised and this text removed..

Comment Number: 178	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 1.4 Page 4	Comment
	Reference: “Because of the timeframe for developing the document, the tasks listed below will be performed in parallel” Working on things in parallel works best for tasks which have little interdependency or relationship. These tasks are clearly highly interdependent and although there is a "significant interaction" it seems likely that the timeframe may have compromised the quality of analysis for this document.
	Rationale/Recommendation

<table>
<tr><td colspan="2">Comment Number: 178</td><td>Submitted by: Elster Electric</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="3"></td><td colspan="3">Although a great deal has been done to generate its contents, more synthesis is clearly needed to make it more coherent, practical and usable.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">Because of the tight time schedule, tasks are being done in parallel. The SGIP-CSWG recognizes the impact this may have and is working hard to ensure the quality is at a high level.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 179</td><td>Submitted by: Elster Electric</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference: 1.4.1</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Reference: “The set of use cases provides a common framework for performing the risk assessment,”
This is only correct if a truly representative set of use cases was chosen. Because neither the generation nor selection of use cases was not done openly, the risk is that the resulting compilation does not adequately represent the entire grid.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The use cases presented in the document are neither exhaustive nor complete. New use cases may be added as they evolve in future versions of this document. The use cases were derived “as-is” from their sources and put into a common format for evaluating Smart Grid characteristics and associated cyber security objectives, requirements and stakeholder concerns.
Anyone may participate in the SGIP-CSWG and the selection of the Use Cases was done in an open process.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 180</td><td>Submitted by: Elster Electric</td><td>Comment Type: __ Technical _X_ Editorial __ General</td></tr>
<tr><td rowspan="2">Reference: 1.4.2</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Reference: “will be done”
Use of future tense, present tense and past tense in various places in the document is only a minor nit, but</td></tr>
</table>

Comment Number: 180	Submitted by: Elster Electric	Comment Type: __ Technical _X_ Editorial __ General
	represents one of the many "rough edges" that result from a rushed process.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR was revised to ensure the use of the proper tense.	

Comment Number: 181	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.4.3 Page 6	Comment	
	Reference: “For each logical interface category, constraints, issues, and impacts were selected using the information provided for each individual interface.” The impacts, in particular are problematic, because they embody an assumption that particular risks are associated with particular interfaces. A more accurate way to view things may be to note that the security risks and impacts don't depend on the interface, but the purpose for which the interface is used. For example, the actual practical institutional importance of say, a padlock on a chain link fence depends not on the fence-padlock interface but what's behind the fence and the level of protection it needs.	
	Rationale/Recommendation	
	None	
	Disposition	
	In the second draft of the NISTIR this list has been removed. Attributes are identified in logical interface categories.	

Comment Number: 182	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 1.4.3 Page 6	Comment	
	Reference: “(Note: this task has not been initiated; therefore, how the security requirements will be allocated has not been finalized.) “ From a practical view, this is one of the more important considerations regarding cyber security.	

Comment Number: 182	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
	Rationale/Recommendation	
	For that reason, and because these allocations will need to be tailored to individual installations, systems and devices, a better approach may be to provide guidelines for rationally performing such allocations without attempting to do so in the abstract.	
	Disposition	
	This language has been removed in the second draft of the NISTIR.	

Comment Number: 183	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.4.4 Page 6	Comment	
	Reference: “NERC CIP 002, 003-009”	
	Rationale/Recommendation	
	Need to cite which version, since it is currently undergoing revision.	
	Disposition	
	The second draft of the NISTIR has been revised to include the version number. Future NISTIR drafts will cite the version of a reference.	

Comment Number: 184	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 2.2 Page 8	Comment	
	Reference: “The lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed.” This is a very good point and is an area in which the federal government could be particularly effective. Simply cataloging the various regulatory requirements regarding privacy protections would not only be extremely useful in itself, but would likely suggest consolidations that would help assure that citizens in every jurisdiction are accorded sufficient privacy protections.	
	Rationale/Recommendation	
	None	

Comment Number: 184	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
	Disposition	
	This will be considered for the next draft of the NISTIR.	

Comment Number: 185	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 2.4 Page 11	Comment	
	Reference: “data automatically collected from smart” The privacy considerations regarding smart meter data are important, but this section of the document seems exclusively focused on meter data. This focus is likely misplaced since much more commonly, the bulk of individuals' PII is not in the meter but within the utilities billing system. Meters don't receive, transmit or store bank account numbers, but billing systems often have exactly that kind of information.	
	Rationale/Recommendation	
	None	
	Disposition	
	The chapter on privacy in the second draft of the NISTIR has been significantly re-written, and now addresses both energy usage data and personal information rather than a focus on smart meter data..	

Comment Number: 186	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 2.4 Page 11	Comment	
	Reference: “Data will flow between the many components”	
	Rationale/Recommendation	
	Change this to “Data will flow among the many components”	
	Disposition	
	This referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 187	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 2.5	Comment	
	Reference: “Automated Smart Grid decisions made for home energy use could be detrimental for residents (e.g.,	

Comment Number: 187	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Page 13	restricted power, thermostats turned to dangerous levels), while decisions about Smart Grid power use and activities could be based upon inaccurate information.” This is a potential risk, but not a privacy risk.	
	Rationale/Recommendation	
	None	
	Disposition	
	The referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 188	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 3.3 Page 20	Comment	
	Reference: “There are critical and non-critical control systems. The requirements for availability will vary depending on a system’s criticality and its impact on the power system.” This is an illustration of why assigning "Low", "Medium", and "High" to an interface is not particularly accurate or useful. The impact depends not on the interface, but the use to which it is put as this note acknowledges.	
	Rationale/Recommendation	
	None	
	Disposition	
	The referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 189	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 3.3 Page 21	Comment	
	Reference: Under Availability, “medium to low impact depending” This somewhat contradicts the column to the left which assigns it "medium" impact. Again, this shows that the only accurate answer to "what is the impact?" may well be "It depends..."	
	Rationale/Recommendation	
	Rather than assigning impacts to interfaces, which is probably misplaced, it may be more useful to outline a	

Comment Number: 189	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
	method by which impacts can be assessed for actual systems and devices rather than trying to assign these in the abstract.	
	Disposition	
	The referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 190	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 3.3 Page 24	Comment	
	Reference: Category 6/Overall Impacts/Availability • Low availability can impact the quality of DMS/EMS actions, leading to inefficient system operation • Loss of electric network “observability “ • May impact customer’s access to data These effects don't seem to merit a "High" impact rating.	
	Rationale/Recommendation	
	None	
	Disposition	
	Availability is now moderate in the second draft of the NISTIR.	

Comment Number: 191	Submitted by: Elster Electric	Comment Type: _X Technical __ Editorial __ General
Reference: Section 3.3 Page 25	Comment	
	Reference: Category 7/Overall Impacts/Confidentiality. • Sensitive customer information is transmitted through some of these interfaces The risk is that customer privacy is breached. The way it's currently phrased, it describes the normal operation but not the impact or risk.	
	Rationale/Recommendation	
	None	
	Disposition	
	Confidentiality is now low in the second draft of the NISTIR.	

Comment Number: 192 | Submitted by: Elster Electric | Comment Type: _X_ Technical __ Editorial _ General

Reference:
Section 3.3
Page 25

Comment

Reference: Category 7/Overall Impacts/Confidentiality.

- Low availability can impact the quality of DMS/EMS actions, leading to inefficient system operation
- Loss of electric network “observability “
- May impact customer’s access to data

These effects don't seem to merit a "High" impact rating.

Rationale/Recommendation

None

Disposition

Confidentiality is now low in the second draft of the NISTIR.

Comment Number: 193 | Submitted by: Elster Electric | Comment Type: _X_ Technical __ Editorial _ General

Reference:
Section 3.3
Page 26

Comment

Reference: Category 8/Overall Impacts/Availability
“Losing one site will not necessarily cause a severe adverse affect to the broader power system.”

This effect doesn't seem to merit a "Medium" impact rating. If a single transformer temperature sensor fails, the impact is probably not "serious" as required in the definition since this is, by definition (as contrasted with Category 9) not a control system, meaning that the transformer could fail with or without a working temperature sensor.

Rationale/Recommendation

None

Disposition

Availability is “moderate” in the second draft of the NISTIR. We will further evaluate for the next version.

Comment Number: 194 | Submitted by: Elster Electric | Comment Type: _X_ Technical __ Editorial __ General

Reference:

Comment

Comment Number: 194	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Section 3.3 Page 28	Reference: Category 10/Overall Impacts/Confidentiality "L-M" These ranges show that this kind of impact categorization is neither practical nor particularly useful as guidance.
	Rationale/Recommendation
	None
	Disposition
	This was split into 10a and 10b to make it more practical in the second draft of the NISTIR.

Comment Number: 195	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 3.3 Page 29, 30	Comment
	Reference: Category 11/Overall Impacts/Integrity Category 12/Overall Impacts/Integrity Category 12/Overall Impacts/Availability "L-H" Another example that shows that this kind of impact categorization is neither practical nor particularly useful as guidance.
	Rationale/Recommendation
	None
	Disposition
	We are now including only one impact level for integrity and availability.

Comment Number: 196	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 3.4 Page 34	Comment
	Reference: Category 10, AMI26; AMI27; AMI29

Comment Number: 196	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
	If AMI26, which does not traverse the AMI network but may cause traffic over the AMI network, is included, why are AMI6, AMI10, AMI11, AMI12 and AMI40 excluded?	
	Rationale/Recommendation	
	None	
	Disposition	
	The architecture diagrams have been updated in the second draft of the NISTIR.	

Comment Number: 197	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 56	Comment	
	Reference to “DHS Catalog of Control Systems Security” This is a misapplication of requirements, since that document describes control systems which it says includes “Supervisory Control and Data Acquisition Systems, Process Control Systems, Distributed Control Systems, and other control systems specific to any of the critical infrastructure industry sectors." AMI systems are typically not control systems in the sense used in the DHS document and so the application of these requirements to such systems may be inappropriate in that the risks are different. AMI systems and SCADA systems are two different realms. The failure to make this distinction results in over specifying controls resulting in the misallocation of limited resources to address problems that are overstated. Simply substituting "AMI" for the word "control" and otherwise copying verbatim most of the DHS document is not as helpful as simply referring the reader to that other document and describing the necessary differences between the kinds of systems and their security requirements.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 198	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 4.1 Page 57	Comment
	“Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses or protocol ports (e.g., TCP ports), combinations of these methods, or other methods as appropriate.” These recommendations fail to reduce risk. Having, for example, the configuration and data acquisition on different TCP ports doesn't really reduce the risk to the port that has the management functions unless some additional action is taken. The security, therefore, is dependent not on the separation of ports, but the additional actions such as firewall blocking, additional logging and auditing, etc. It's understood that this text comes largely from the DHS Catalog.
	Rationale/Recommendation
	None
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 199	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 4.1 Page 58	Comment
	“The AMI system maintains a separate execution domain (e.g., address space) for each executing process.” Taking a recommendation originally intended for SCADA systems and applying them to AMI systems (where there is commonly a 100:1 or more cost ratio for field devices) has a deleterious effect on overall grid security because it 1) ignores the very real difference between the different kinds of systems and 2) may induce utilities to misapply their limited funds attempting to redress the wrong problems.
	Rationale/Recommendation
	None
	Disposition

Comment Number: 199	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 200	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 4.1 Page 58	Comment
	"Passwords and/or security keys should be of limited value, avoiding significant reuse of keys or passwords between different components and users. For example, compromising one key must not allow compromise of an entire network." This item is misplaced because it does not describe an aspect of security function isolation, but rather the handling and use of cryptographic material.
	Rationale/Recommendation
	None
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 201	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 4.1 Page 59	Comment
	DHS-2.8.5.2 Supplemental Guidance: "Wireless assets and networks are also vulnerable to radio-frequency jamming and steps must be taken and personnel trained to address tracking and resolution of such issues. This may include radio-frequency direction finding and other such technologies." Wired systems are vulnerable to wire cutters, but we don't call that out as a separate item and don't suggest that

<table>
<tr><td>Comment Number: 201</td><td colspan="2">Submitted by: Elster Electric</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5"></td><td colspan="3">utility personnel be training in using Time Domain Reflectometry (TDR) to locate the cut or in forensically examing tool marks to determine exactly how a wire was cut. This is just silly and should be deleted.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.</td></tr>
</table>

<table>
<tr><td>Comment Number: 202</td><td colspan="2">Submitted by: Elster Electric</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Section 4.1
Page 60</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">DHS-2.8.6.2 Supplemental Guidance: “This control does not apply to components in the system for which only a single user/role exists. “

When this was copied from the DHS document, this sentence was omitted. Pointing out situations in which the control does NOT apply is, unfortunately, a systeming problem for this entire section. The DHS catalog is just that -- a catalog -- and like any catalog, it is expected that some discernment is required. Choosing everything is to make no choice at all and to simply shift the engineering burden to the implementers and the cost ultimately the consumers of electricity who will ultimately pay for a bloated and over specified system if we allow it to exist. This weakens rather than enhances Smart Grid security because it encourages (requires?) squandering resources on the wrong security issues.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.</td></tr>
</table>

Comment Number: 203	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 60	Comment	
	DHS-2.8.7.2 Supplemental Guidance: “The HAN is not controlled or owned by the utility, and should be treated as a hostile network by the AMI meter.” This statement goes well outside the scope of providing a "conceptual architecture" into dictating the business and technical outlines of the Smart Grid.	
	Rationale/Recommendation	
	To acknowledge that this is only one possibility, the statement was changed to a conditional predicate: “In the case that the HAN is not controlled or owned by the utility…”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 204	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 60	Comment	
	DHS-2.8.7.2 Supplemental Guidance: “Because of this, we recommend that AMI components should not request or accept information from HAN components.” This is a faulty recommendation because it ignores many different kinds of use cases, such as transmitting the positive acknowledgement by a utility customer of a demand response signal, the existence of and state of charge of a PHEV, and even the simplest of signals such as that which indicates that the HAN even exists. All of these require that information flow from the HAN toward the utility.	
	Rationale/Recommendation	
	None	
	Disposition	

Comment Number: 204	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 205	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 60	Comment	
	DHS-2.8.7.2 Supplemental Guidance: “Generally, no AMI system information should be publicly accessible” This is another illustration of the problem with cut-and-paste requirements. In fact, much of the point to the Smart Grid is to make AMI system information publically availaible so that consumers of energy (i.e. the public) can more effectively manage their own energy usage, so not only is this guidance of dubious value, but its premise is demonstrably false.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 206	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 60	Comment	
	DHS-2.8.7.2 Supplemental Guidance: “Field service tools should not interface to the meter through the HAN.” A good requirement should state what is needed or is to be accomplished but avoid dictating design or implementation details. This requirement both fails to state what is needed and only dictates a design detail.	

Comment Number: 206	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

	Rationale/Recommendation
	None
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 207	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 4.1 Page 60	Comment
	DHS-2.8.7.2 Supplemental Guidance: "The organization shall limit the number of access points to the AMI system to allow for better monitoring of inbound and outbound network traffic" A good requirement should state what is needed or is to be accomplished but avoid dictating design or implementation details. This requirement both fails to state what is needed (better monitoring? compared with what?) and only dictates a design detail.
	Rationale/Recommendation
	None
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 208	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Reference:	Comment

Comment Number: 208

Submitted by: Elster Electric

Comment Type: _X_ Technical __ Editorial __ General

Section 4.1
Page 60

DHS-2.8.7.2 Supplemental Guidance:

- The organization prevents the unauthorized ex-filtration of information across managed interfaces.
- The control system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
- The control system at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external systems.
- The control system prevents remote devices that have established a nonremote connection with the system from communicating outside that communications path with resources in nonorganization controlled networks.
- The control system routes all internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices.

If we're going to cut and paste, let's not miss guidance that might actually be useful and relevant.

Rationale/Recommendation

None

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 209

Submitted by: Elster Electric

Comment Type: _X_ Technical __ Editorial __ General

Reference:
Section 4.1
Page 61

Comment

DHS-2.8.8.2 Supplemental Guidance: “Contracts and other legal documents with vendor should allow for security and integrity testing of products and services used in the AMI system Contracts and other legal documents with vendors should allow for security and integrity testing of products and services used in the AMI systems.”

Comment Number: 209	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
	This is dictating a business practice and is inappropriate for this document. Security and integrity testing might or might not be the "appropriate contracting vehicle" chosen.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 210	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 61	Comment	
	DHS-2.8.8.3 Requirement Enhancements: “The control system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.” This was omitted when cut and pasted from the DHS document. It applies just as much to an AMI system as to a control system, since faithfully returning unaltered data from the field is, in fact, most often the primary purpose for an AMI system.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 211	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 211	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 62	Comment	
	DHS-2.8.10.2 Supplemental Guidance: “It is recommended that login to the field service tool interface be protected by a trusted path or a compensating control.” If a trusted path does not exist, what compensating control could possibly be useful? By definition, the failure of a trusted path means that security guarantees can no longer be trusted.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 212	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 63	Comment	
	DHS-2.8.13/ NIST SP 800-53 SC-15 Collaborative Computing: Referring to the “N/A” at then end of the subsection title. This same tag could and perhaps should be applied to many of the provisions in this document.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 213	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 64	Comment	
	DHS-2.8.14.3 Requirement Enhancements: "The control system validates the integrity of security parameters exchanged between systems" This was omitted from the cut and paste from the DHS document but seems fundamental.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 214	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 66	Comment	
	DHS-2.8.19.2 Supplemental Guidance:" Security roles and responsibilities for AMI system users must be specified, defined, and implemented based on the sensitivity of the information handled by the AMI system." The DHS document from which this was cut and pasted said "user" here and not system. This substitution changes the meaning substantially and makes it less sensible.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 215	Submitted by: Elster Electric	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 4.1 Page 68	Comment	
	ASAP-2.8.24.2 Supplemental Guidance: “Appropriate components or programming must be included within the AMI networks to identify potentially malicious address-resolution behavior (eg. ARP spoofing/cache poisoning). Such behavior should be identified, tracked, and the appropriate incident handling team-members alerted.” This supplemental guidance offers no real guidance. What are “appropriate components or programming" and how would one objectively evaluate this? Further, is it sufficient to merely identify such an attack, or is there a more direct mitigation that could/should be applied?	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 216	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.3 Page 2	Comment	
	Reference: “With the adoption and implementation of the Smart Grid, the IT and telecommunication sectors will be more directly involved. These sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in these systems.” Business IT application and network organizations may or may not be directly involved depending on utility structure. IT technologies may be applied and managed by utility operations. Smart Grids may not necessarily share IT networks.	
	Rationale/Recommendation	
	Change above referenced text to read: “With the adoption and implementation of the Smart Grid with off the shelf IT technology, telecommunication sector will be more directly involved. Existing cyber security standards to address	

Comment Number: 216	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
	vulnerabilities and assessment programs can help identify known vulnerabilities in these systems. “	
	Disposition	
	This section was updated to reflect the suggested changes.	

Comment Number: 217	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.4 Page 6	Comment	
	Reference: “The Smart Grid security architecture will overlay this conceptual architecture and security requirements will be allocated to specific domains, mission/business functions and/or interfaces included in the Smart Grid conceptual reference model. “ Which specific domains?	
	Rationale/Recommendation	
	None	
	Disposition	
	This section has been revised in the second draft of the NISTIR. NIST SGIP-CSWG is addressing the entire Smart Grid.	

Comment Number: 218	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 1.4 Page 6	Comment	
	Reference: “NERC CIP 002, 003-009” How does the Smart Grid distribution system fall under the jurisdiction of NERC and bulk power rules?	
	Rationale/Recommendation	
	None	
	Disposition	
	The NISTIR addresses the entire Smart Grid. Any questions related to the role of NERC should be forwarded to	

Comment Number: 218	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

	that organization.

Comment Number: 219	Submitted by: Hawaiian Electrical Company	Comment Type: __ Technical _X_ Editorial __ General

Reference: Section 2.4 Page 10	Comment
	Reference: “from large generation power transmission” Should there be a comma between the words power and transmission?
	Rationale/Recommendation
	None
	Disposition
	The referenced text was removed from the second draft of the NISTIR.

Comment Number: 220	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 3.1 Page 15	Comment
	Reference: “1. Control systems with high data accuracy and high availability, as well as media and compute constraints” It is not clear what is meant by "as well as media and compute constraints"
	Rationale/Recommendation
	None
	Disposition
	The logical interface descriptions have been revised in the second draft of the NISTIR to include additional descriptive information.

Comment Number: 221	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 221	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.1 Page 15	Comment	
	Reference: “2. Control systems with no bandwidth constraints wide area network (WAN) but are in different organizations” No bandwidth constraints because it uses a WAN between the two systems or because less data is shared?	
	Rationale/Recommendation	
	None	
	Disposition	
	Referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 222	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.1 Page 16	Comment	
	Reference: “9. Interfaces between sensor networks and control systems” Is the difference between this category #9 and category #1 that field device is only a sensor (no controls) or more the type of control system?	
	Rationale/Recommendation	
	None	
	Disposition	
	Yes. #9 is sensor only with no controls. #1 has been expanded and includes more detail.	

Comment Number: 223	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.3 Page 23	Comment	
	Reference: “Cross-organizational interactions, which limit trust and compatibility of security policies and measures.”	

Comment Number: 223	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

	Is this an issue or constraint? Constraints should be very similar to Category 4?
	Rationale/Recommendation
	None
	Disposition
	The reference to logical interface category # 5 has been removed. Logical interface categories are now being defined by attributes that include constraints, issues, and requirements.

Comment Number: 224	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 3.3 Page 26	Comment
	Reference : "Category 9" Should this category be moved next to Category #1? The only difference seems to be the availability of the control system.
	Rationale/Recommendation
	None
	Disposition
	Logical interface categories are in no particular order. #9 is sensor only with no controls. #1 has been expanded with more details in the second draft of the NISTIR.

Comment Number: 225	Submitted by: Hawaiian Electrical Company	Comment Type: __ Technical _X_ Editorial __ General

Reference: Section 3.3. Page 27	Comment
	Reference: "Category 9/Constraints"
	Rationale/Recommendation
	Add the following bullets to the list of constraints for category 9:

Comment Number: 225	Submitted by: Hawaiian Electrical Company	Comment Type: __ Technical _X_ Editorial __ General

	• Many devices have no notion of a user or a role making security management a challenge. • Often no security event information available from these systems • No standard for security events or logging
	Disposition
	In the second draft of the NISTIR attributes, including constraints, are specified for the logical interface categories.

Comment Number: 226	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 3.3 Page 27	Comment
	Are Category #9 control systems considered all “non-critical”?
	Rationale/Recommendation
	None
	Disposition
	All the logical interface categories have been revised in the second draft of the NISTIR. The focus of the NISTIR was to identify security requirements for the entire Smart Grid, not focusing on the criticality of systems.

Comment Number: 227	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 3.3 Page 28	Comment
	Reference: “Category 10 - Interfaces that use the AMI network” Can a Category 10 also be a Category 12?
	Rationale/Recommendation
	None
	Disposition
	Logical interface category definitions have been updated to avoid confusion in the second draft of the NISTIR.

Comment Number: 227	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
	Each logical interface is included in only one logical interface category.	

Comment Number: 228	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.3 Page 28	Comment	
	Reference: “Category 10/Constraints” If no defined constraints and issues, this may be covered by Category #12? The overall impacts seem to overlap with Category #12? Is this a subset of #12?	
	Rationale/Recommendation	
	None	
	Disposition	
	Logical interface category definitions have been updated to avoid confusion in the second draft of the NISTIR.	

Comment Number: 229	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.3 Page 34	Comment	
	Suggest added section on assumptions of systems/applications before the six functional area diagrams used in all logical interface categories: • Control systems: o Utility EMS o OMS application o AMI Head-end o Distribution SCADA o OMS • Control systems in different organizations: o Utility EMS and Dist SCADA o Utility EMS and OMS • Control systems in same organizations: o OMS; Distribution SCADA, Load Mgmt System	

<table>
<tr><td>Comment Number: 229</td><td>Submitted by: Hawaiian Electrical Company</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5"></td><td colspan="2">• Back office systems:
o AMI
o CIS
o MDMS

This will help make reviewing all the diagrams and make use of categories more consistent.</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">None</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">Description of actors have been more clearly defined in the second draft of the NISTIR.</td></tr>
</table>

<table>
<tr><td>Comment Number: 230</td><td>Submitted by: Hawaiian Electrical Company</td><td>Comment Type: _X Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Section 3.4
Page 34</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">Reference: “Category 1/Logical Interfaces”

Should this [AMI40] be Category 9? Is AMI high availability and real time?</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">None</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">Logical interface category definitions have been updated to avoid confusion in the second draft of the NISTIR.</td></tr>
</table>

<table>
<tr><td>Comment Number: 231</td><td>Submitted by: Hawaiian Electrical Company</td><td>Comment Type: _X Technical __ Editorial __ General</td></tr>
<tr><td rowspan="3">Reference:
Section 3.4
Page 34</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">Reference: “ Category 10/Interfaces that use the AMI network”

Why was this a separate category? Does it need a separate solution? Is Category 10 a subset of other Categories (i.e., #4 or #5)?</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
</table>

Comment Number: 231	Submitted by: Hawaiian Electrical Company	Comment Type: _X Technical __ Editorial __ General
	None	
	Disposition	
	Logical interface category definitions have been updated to avoid confusion in the second draft of the NISTIR.	

Comment Number: 232	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.5 Page 37	Comment	
	Reference: " Category 4/Back office systems under common management authority /Logical Interfaces/DGM31 discrepancy with 3.4 AMI6?	
	Rationale/Recommendation	
	None	
	Disposition	
	Diagrams have been updated in the second draft of the NISTIR.	

Comment Number: 233	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.5 Page 37	Comment	
	Reference: " Category 10/Interfaces that use the AMI network/Logical Interfaces/DGM31 How is this different from Category 4?	
	Rationale/Recommendation	
	None	
	Disposition	
	Logical interface category 4 has been removed in the second draft of the NISTIR.	

Comment Number: 234	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 234	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.5 Page 38	Comment	
	Reference: “ Category 12/Interface to the Customer Site/Logical Interfaces/DGM13 Is this correct?	
	Rationale/Recommendation	
	None	
	Disposition	
	The diagrams have been updated in the second draft of the NISTIR. An overall functional logical architecture is now included in the document.	

Comment Number: 235	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 3.5 Page 38	Comment	
	Reference: “ Category 12/Interface to the Customer Site/Logical Interfaces/DGM23 I can’t find DGM23 in diagram.	
	Rationale/Recommendation	
	None	
	Disposition	
	The diagrams have been updated in the second draft of the NISTIR. An overall functional logical architecture is now included in the document.	

Comment Number: 235	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix A Page A-1	Comment	
	Reference: Appendix A Should the Use Cases have references back to the AMI Requirements listed in Chapter 4?	

Comment Number: 235	Submitted by: Hawaiian Electrical Company	Comment Type: _X_ Technical __ Editorial __ General
	Rationale/Recommendation	
	None	
	Disposition	
	The final version of the NISTIR will include design considerations to assist people in use of the document.	

Comment Number: 236	Submitted by: PEPCO	Comment Type: __ Technical __ Editorial _X_ General
Reference: Chapter 1	Comment	
	PHI recommends that this document be revised so that it is consistent with the "NIST Framework and Roadmap for Smart Grid Interoperability Standards". The document needs to be revised in a cohesive manner that clearly articulates a strategy for Smart Grid Cyber Security.	
	Rationale/Recommendation	
	None	
	Disposition	
	The cyber security strategy in the NIST Framework and the NISTIR are the same.	

Comment Number: 237	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 1	Comment	
	The definition of Cyber Security should be modified so that it is more specifically relevant to the electric utility industry. The document covers predominately the AMI portion of the Smart Grid and should provide details for the other components of the Smart Grid (i.e. Distribution Applications, smart substations, Capacitor Bank Controllers, Smart Relays, etc.) This list is only representative of the devices which describe the Smart Grid.	
	Rationale/Recommendation	
	None	
	Disposition	
	The definition of cyber security has been revised to be more inclusive of the information technology,	

Comment Number: 237	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
	telecommunications, and electric sectors. The emphasis of the NISTIR is on overall requirements for the Smart Grid and diverse pathways and redundancy are potential controls to meet these requirements.	

Comment Number: 238	Submitted by: PEPCO	Comment Type: __ Technical __ Editorial _X_ General
Reference: Chapter 1	Comment	
	PHI is requesting that NIST further define how the NERC CIP standards 002-009 will apply to the Smart Grid. These standards currently apply to the bulk power system and it would be costly to apply it to all of the AMI and Distribution systems.	
	Rationale/Recommendation	
	None	
	Disposition	
	The NERC CIPs are mandatory for the bulk power system. The specific requirements in the NERC CIPs are being reviewed for inclusion in the NISTIR.	

Comment Number: 239	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 1	Comment	
	PHI understands the immediate need to develop standards for the Smart Grid, including specifically security requirements. PHI believes that the timeline is extremely aggressive and driving this to too quick a conclusion could produce inferior standards, requirements and/or strategies.	
	Rationale/Recommendation	
	None	
	Disposition	
	Because of the tight time schedule, tasks are being done in parallel. The SGIP-CSWG recognizes the impact this may have and is working hard to ensure the quality is at a high level.	

Comment Number: 240	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 2.5.6	Comment	
	PHI agrees that the "lack of consistent and comprehensive privacy policies, standards, and supporting procedures [on] information collection and use creates a privacy risk that needs to be addressed." Many of NISTIR 7628's recommendations provide excellent strategies for mitigating such risks.	
	Rationale/Recommendation	
	None	
	Disposition	
	Thank you for the comment.	

Comment Number: 241	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 2.5.1, 2.5.6 and 2.5.9	Comment	
	Utility companies should develop policies to determine what customer information should be confidential, how that information should be retained, distributed internally and secured from breach. As noted in § 2.5.1, training employees is critical to implementing this policy. Similarly, customers should be informed as to what information the utility company is collecting and how that information will be used. Customers should also be able to inspect that information for accuracy and quality as recommended by §§ 2.5.6 and 2.5.9.	
	Rationale/Recommendation	
	None	
	Disposition	
	The privacy section has been revised to include privacy practices that address these concerns.	

Comment Number: 242	Submitted by: PEPCO	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	In order to promote customer service, a customer's information must be available for all utility company employees who need to provide services in addition to billing and rendering. Smart meters give customer service personnel the opportunity to provide individual guidance on managing energy use which would be difficult and less effectual if those	

Comment Number: 242	Submitted by: PEPCO	Comment Type: __ Technical __ Editorial _X_ General

	employees are unable to access a customer's information. Similarly, maintenance personnel may need access to that information in order to perform repairs. It is important that internal movement of information is not hindered by overly restrictive policies or regulations.
	Rationale/Recommendation
	None
	Disposition
	The NISTIR includes recommended privacy practices and security requirements, including the development of policies. The development of regulations is outside the scope of the SGIP-CSWG.

Comment Number: 243	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General

Reference: Sections 2.5.4 and 2.5.7	Comment
	Currently, information collected by utility companies to initiate service is regulated by tariffs filed with the applicable state public service commission (PSC). The current process for tariff approval adequately considers customer privacy. Similarly, states such as Maryland require a public filing for a small generation interconnection request. See COMAR 20.50.09.06. Utility companies must comply with that regulation which requires disclosure of information that would normally be considered PII. There appears to be a disconnect between § 2.5.4 that recognizes that this information is collected and § 2.5.7 which does not seem to recognize that it is disclosed.
	Rationale/Recommendation
	Proposed language would be: “Disclosure and Limiting Use: PII should be used only for the purposes for which it was collected. PII should not be disclosed to any other parties except as required by law, regulation or policy on file with the state public service commission upon disclosure of that policy to the individual whose PII could be disclosed.”
	Disposition
	The privacy section has been revised to include privacy practices that address these concerns.

Comment Number: 244	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General

Reference:	Comment

Comment Number: 244	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Chapter 3	PHI recommends that this section be moved to the appendices portion of the document and that it be re-titled to Proposed Logical Interfaces. Because utilities have made large investments in key systems each utility's Smart Grid systems may be architected differently. The proposal provides a "one size fits all" approach. An example of this single architecture approach is demonstrated in diagram 3.5. This diagram implies that the DMS functions are DOMA, VVWS, FLIR, MFR, OMS, WMS, etc. This may not be the case for all DMS systems. Also, most utilities use standalone OMS systems.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has been revised to clarify that these are logical interface diagrams are not solutions and they do not imply any physical architectures.	

Comment Number: 245	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	The draft NISTIR states the "Connections to the Internet and other public networks is discouraged for AMI systems." This statement appears to severely limit the communication options for this interface. Many proposed and deployed solutions use the public internet as the transport to access points for their AMI solution.	
	Rationale/Recommendation	
	Focus should be applied on how to secure the transported information through the internet rather than discourage its use.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 246	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 246	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	The Draft NISIR proposes that "AMI components should only push traffic to the home area network."	
	Rationale/Recommendation	
	PHI suggests that this language be revised to allow two way communications to the HAN. In any case, some HAN devices will be required to register to the Smart Meter, thus requiring two way communications.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 247	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	PHI also suggests that the Smart Grid Cyber Security Strategy and Requirements Document provide a clear strategy and a "tool kit" that provides both guidance and methods to resolve conflicts between operability and security requirements for all stakeholders. In order to assist the utilities in accomplishing the requirements or strategies, it would be beneficial to create a list or summary of guiding principles.	
	Rationale/Recommendation	
	None	
	Disposition	
	The focus of this NISTIR is on high-level security requirements and does not address security solutions.	

Comment Number: 248	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	PHI is not clear on the intent of the Smart Grid Cyber Security Strategy and Requirements Document as it relates to regulatory requirements. The NIST Framework and Roadmap document indicates that, once consensus is	

Comment Number: 248	Submitted by: PEPCO	Comment Type: _X_ Technical __ Editorial __ General
	achieved, FERC will use its rule making authority to adopt the necessary standards and protocols for Smart Grid implementation. This process requires additional clarification for the utilities.	
	Rationale/Recommendation	
	None	
	Disposition	
	Regulation and jurisdiction are outside the scope of the SGIP-CSWG. NIST is working closely with FERC, NARUC, and the PUCs on the use of the NIST documents.	

Comment Number: 249	Submitted by: PEPCO	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	In order to increase clarity of the documents, PHI suggests that a glossary is provided which defines all acronyms, key elements and terms.	
	Rationale/Recommendation	
	None	
	Disposition	
	Appendix F of the second draft of the NISTIR contains an updated glossary and acronym list.	

Comment Number: 250	Submitted by: SEL	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	The user guide could take many forms, but one suggestion is to provide one or more step-by-step guide(s) to illustrate how it could be used by utilities and their vendors. Another possibility is a decision tree that directs the reader to the relevant portions of the document for information. It will also be helpful for the user guide to state that there is no single "one-size-fits-all" security solution; and that each project needs to be evaluated individually to incorporate appropriate security controls.	
	Rationale/Recommendation	
	Incorporate a brief user guide to make the NISTIR more approachable.	

Comment Number: 250	Submitted by: SEL	Comment Type: __ Technical __ Editorial _X General
	Disposition	
	The final version of the NISTIR will include design considerations to assist people in the use of the document.	

Comment Number: 251	Submitted by: SEL	Comment Type: _X_ Technical __ Editorial _ General
Reference: 1.2 & 1.3	Comment	
	Cyber security in the context of power systems is different than cyber security of corporate networks and other IT systems. Electric utilities are accountable for power system safety and reliability, and cyber security of power systems must always be placed into that context. Because not all of the readers of this document will have this fundamental knowledge, such a discussion is important to avoid misinterpretations of the material and to ensure that all stakeholders have a common frame of reference for the recommendations in the NISTIR.	
	Rationale/Recommendation	
	Add a paragraph or two in section 1.2 or 1.3 that puts cybersecurity into its appropriate context in electric power systems, which is as a component of power system reliability and something that must support safety and reliability but should not compromise either.	
	Disposition	
	We have revised the definition of cyber security to be more inclusive of the IT, Telecommunications, and electric sectors. In addition, the strategy has been expanded to clarify the importance of power system reliability.	

Comment Number: 252	Submitted by: SEL	Comment Type: __ Technical __ Editorial _X General
Reference: Overall	Comment	
	A clearly defined scope will help set the reader's expectations, and will also help the authors of the document by reducing the inclination to try to be exhaustive. There is a psychology barrier associated with a 200-plus page document. Bearing in mind how the document will be used by utilities and Smart Grid suppliers, NIST should resist being exhaustive in scope, in favor of being sufficiently clear within the scope described above. Anything that reduces barriers to using the information in the NISTIR, including increased clarity and manageable volume, will likely be helpful to improving cybersecurity.	
	Rationale/Recommendation	
	The scope of the document should be limited to recommending cybersecurity controls for the Smart Grid applications we know of today (by listing the use cases). The "Overview" section (currently section 1.1) of the final document should define the scope of the document.	

Comment Number: 252	Submitted by: SEL	Comment Type: __ Technical __ Editorial _X General
	Disposition	
	We have revised section 1 and included a scope. The final version of the NISTIR will include design considerations to assist people in the use of the document.	

Comment Number: 253	Submitted by: SEL	Comment Type: __ Technical __ Editorial _X General
Reference: 1.1	Comment	
	Given that one of the policy objectives of EISE is innovation, it is possible that new interfaces, categories of interfaces, as well as impacts and constraints may arise, while other categories, constraints, and impacts may diminish in importance. Neither NIST nor any of the stakeholders involved in writing the NISTIR can foresee every security consideration that may arise, and therefore, the NISTIR is limited in describing recommended security considerations and appropriate controls to be considered for 18(?) categories of interfaces that we believe capture the vast majority of Smart Grid projects envisioned today.	
	Rationale/Recommendation	
	Be explicit in the Overview about indicating that the document is not exhaustive, and about deliberately excluding certain topics, such as physical security.	
	Disposition	
	Have revised the second draft of the NISTIR to clarify that the document is neither final nor comprehensive on all topics.	

Comment Number: 254	Submitted by: SEL	Comment Type: __ Technical _X_ Editorial __ General
Reference: Chapter 2	Comment	
	SEL believes that trying to address both cybersecurity and privacy in a single report creates the potential to delay important guidance on cyber security for aspects of Smart Grid architecture that do not involve customer data, and do not, therefore, invoke privacy concerns. Utilities implanting Smart Grid projects with ARRA funding need to have cybersecurity guidance in hand as soon as possible in order to ensure that they are fulfilling their obligations under the terms of the DOE grants. In addition, inclusion of the privacy chapter adds to the volume of the NISTIR, potentially making the document more challenging to use as guidance for the intended audience. Two separate, authoritative reports, each with a clear focus, would likely be more user-friendly.	

Comment Number: 254	Submitted by: SEL	Comment Type: __ Technical _X_ Editorial __ General
	Rationale/Recommendation	
	Consider removing Chapter 2 (on Privacy) from this NISTIR and creating a separate NISTIR or other document to address Smart Grid privacy considerations and recommended approaches.	
	Disposition	
	Privacy is an important topic and is addressed with security in the NISTIR.	

Comment Number: 255	Submitted by: SEL	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Consider other ways to make the document more concise. One possibility for reducing the volume of the document without reducing the content would be to remove the use case diagrams and associated lists categorizing the logical interfaces for each use case, and instead provide a single listing of the categories of logical interfaces with a detailed list of examples for each category, might reduce the redundancy of the document.	
	Rationale/Recommendation	
	None	
	Disposition	
	The final version of the NISTIR will include design considerations to assist people in use of the document.	

Comment Number: 256	Submitted by: SEL	Comment Type: __ Technical _X Editorial __ General
Reference: Overall	Comment	
	Think about ways to create useful job aids for the primary utility Smart Grid supplier audiences. For example, the cross-walk in appendix B is a useful reference that may lend itself to printing separately. Any future formatting of the NISTIR should be done to ensure that a user of the NISTIR could easily print the crosswalk as a handy reference. In addition, there may be other	
	Rationale/Recommendation	
	None	
	Disposition	

Comment Number: 256	Submitted by: SEL	Comment Type: __ Technical _X Editorial __ General
	The comment appears incomplete. Please clarify your question/comment for the next version of the NISTIR.	

*** To pick up and review with Annabelle

Comment Number: 257	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.31 (Page 222)	Comment	
	Local role for emergency actions in the event of loss of connection to centralized authority.	
	Rationale/Recommendation	
	None	
	Disposition	
	Please clarify your question/comment for the next version of the NISTIR.	

Comment Number: 258	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.32 (Page 222)	Comment	
	IDS should also monitor information flows. This may present problems with so many protocols to monitor.	
	Rationale/Recommendation	
	None	
	Disposition	
	There are multiple products that are capable of monitoring many protocols at the same time.	

Comment Number: 259	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.33 (Page 222)	Comment	
	This follows on from point made above	
	Rationale/Recommendation	

Comment Number: 259	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	None	
	Disposition	
	Please clarify your question/comment for the next version of the NISTIR.	

Comment Number: 260	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.34 (Page 222)	Comment	
	This requires a definition of what constitutes a security event in a power system. Interested groups (e.g. PSRC) should be actively involved in this + event type and format definitions.	
	Rationale/Recommendation	
	None	
	Disposition	
	We welcome the participation and input from experts, anyone can join the SGIP-CSWG. Contact Annabelle Lee at: Annabelle.lee@nist.gov	

Comment Number: 261	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.37 (Page 223)	Comment	
	IEC62351-8 recommends time limited credentials which would be one solution to the issue of revocation without a centralized security manager.	
	Rationale/Recommendation	
	None	
	Disposition	
	The NISTIR is developing requirements, not solutions. Please clarify your question/comment for the next version of the NISTIR.	

Comment Number: 262	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.38 (Page 223)	Comment	
	"passwords should be avoided" is OK for equipment where alternative authentication schemes are possible. But many legacy devices will not have such features, and perhaps some suppliers may not be able to deliver equipment with these alternatives (at least in the short term).	
	Rationale/Recommendation	
	None	
	Disposition	
	Recognizing that legacy equipment exists, there is a discussion of compensating controls in the NISTIR. We will include more information on legacy equipment in the next version of the NISTIR.	

Comment Number: 263	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.45 (Page 224)	Comment	
	This is the real issue. It is easy to specify strong security features that fit well with the smart-grid in new equipment, or in firmware upgrades in relatively new equipment that has good resource availability. But relays that are, say, 10+ years old are unlikely to be capable of update, and there will be huge reluctance to change the devices, Legacy devices may not even have any security at all. How these can be brought under a security umbrella is a major consideration.	
	Rationale/Recommendation	
	None	
	Disposition	
	Great points. The Bottom Up group will consider how to accommodate these ideas in the next version of the NISTIR. Please consider joining the Bottom Up conference call and/or email suggestions to csctgbu@nist.gov to aid in developing specific text.	

Comment Number: 264	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 264	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
D.46 (Page 224)	This introduces constraints on the ideal target of being able to address and rectify a known vulnerability. Determining the cost of applying the patch against the benefit of the fix (or the possible cost if the patch is not applied and an attack results) is a tricky business.	
	Rationale/Recommendation	
	None	
	Disposition	
	Great points. The Bottom Up group will consider how to accommodate these ideas in the next version of the NISTIR. Please consider joining the Bottom Up conference call and/or email suggestions to csctgbu@nist.gov to aid in developing specific text.	

Comment Number: 265	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.46 (Page 224)	Comment	
	IEC62351-8 defines some mandatory roles and many different rights, not all of them satisfied by the mandatory roles or the list of roles in D.49.	
	Rationale/Recommendation	
	None	
	Disposition	
	IEC62351-8 is not complete. The roles identified in the NISTIR are not “mandatory”.	

Comment Number: 266	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.53 (Page 227)	Comment	
	As in my point Thompson/02. Reference to comment: “IDS should also monitor information flows. This may present problems with so many protocols to monitor.”	
	Rationale/Recommendation	

Comment Number: 266	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	None	
	Disposition	
	Great points. The Bottom Up group will consider how to accommodate these ideas in the next version of the NISTIR. Please consider joining the Bottom Up conference call and/or email suggestions to csctgbu@nist.gov to aid in developing specific text.	

Comment Number: 267	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.54 (Page 227)	Comment	
	Huge problem with legacy products that have problems and vulnerabilities already, and the issue with patch management and f/w updates already covered.	
	Rationale/Recommendation	
	None	
	Disposition	
	Great points. The Bottom Up group will consider how to accommodate these ideas in the next version of the NISTIR. Please consider joining the Bottom Up conference call and/or email suggestions to csctgbu@nist.gov to aid in developing specific text.	

Comment Number: 268	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 1	Comment	
	"With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information," implies that two-way flow of information was caused by the Smart Grid. This can not be true because two-way flow of information has been around for decades, it has just been very slow. Two way flow of electricity has been around since the beginning of the grid. This is a terrible way to start off the document.	
	Rationale/Recommendation	
	None	
	Disposition	

Comment Number: 268	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	This wording has been updated. The referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 269	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 1	Comment	
	"To achieve this requires that security be designed in at the architectural level." Is "cyber security intended instead of just security?	
	Rationale/Recommendation	
	None	
	Disposition	
	The referenced text has been removed from the second draft of the NISTIR.	

Comment Number: 270	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 6	Comment	
	B2B not defined on page 6. But it is defined later in the document on page 23.	
	Rationale/Recommendation	
	None	
	Disposition	
	This has been corrected in the second draft of the NISTIR.	

Comment Number: 271	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	None	
	Rationale/Recommendation	

Comment Number: 271	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	The AMI-SEC requirements should be included in an informative annex and not in the main body of the document.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 272	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 11	Comment	
	"discussions and speculation about how data automatically collected from smart meters" is limited to only privacy concerns of one element of the Smart Grid. This should be generalized to "discussions and speculation about how data automatically collected from smart devices", because it very well applies to revenue meters, smart thermostats, smart appliances, and any other device networked to support the Smart Grid.	
	Rationale/Recommendation	
	None	
	Disposition	
	The privacy section has been revised and expanded in the second draft of the NISTIR. This text has been removed.	

Comment Number: 273	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 11	Comment	
	"The scope of this PIA is the consumer meter to local utility" is inappropriately included in section 2.4 because privacy concerns extend to more than just meters.	
	Rationale/Recommendation	
	None	
	Disposition	

Comment Number: 273	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	The privacy section has been revised and expanded in the second draft of the NISTIR. This text has been removed.	

Comment Number: 274	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 11	Comment	
	Figure 2.1 completely ignores remote access to devices supporting Smart Grid. The introducing sentence states "information flow" while the title states "information sharing" - these are completely two different items. Flow does not imply or even require sharing.	
	Rationale/Recommendation	
	None	
	Disposition	
	The title of the figure has been changed in the second draft of the NISTIR.	

Comment Number: 275	Submitted by: IEEE	Comment Type: __ Technical _X_ Editorial __ General
Reference: Page 11	Comment	
	"The bi-directional flow of data between utilities and customer premises will now be more similar to the types of data flows between commercial meters and utilities." This sentence assumes that data flow already exists between commercial meters and utilities - this is not the case. Replace "will now be more similar to" with "Is".	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR contains a revised privacy section and this reference has been removed.	

Comment Number: 276	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 276	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Chapter 2	Chapter 2 should relate how the findings in the "high-level PIA of the consumer-to-utility metering data sharing portion of the Smart Grid" can be applied to the whole of the Smart Grid. Otherwise, this whole chapter belongs as an appendix as a summary of those findings. This section on privacy should be based upon that work, not repeat it or be limited by it, as this singular focus leaves out other areas of privacy concerns in Smart Grid.	
	Rationale/Recommendation	
	None	
	Disposition	
	The privacy section has been revised and expanded in the second draft of the NISTIR.	

Comment Number: 277	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 15	Comment	
	The last example on page 15 under Category 7 is not a very good example. Item 7 is "Interfaces between control systems and non-control systems" and the example is "between a Geographic Information System (GIS) and a Load Management/Demand Response (DR) System", where a GIS is not a control system and LMR and DR are not typical examples of a control system. Better examples would be between a control system and a computerized maintenance system, or historian, or remote access system. Unless this item is changed to include remote access systems, a huge gap in use will not be addressed by these standards. Not sure if a separate classification would be required for a separate device in addition to a control system - for example, would a relay sitting at switch location on a distribution feeder be considered a control system - it is only one device, is self contained, and possibly has no other elements involved in control.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised the examples for logical interface category 7.	

Comment Number: 278	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 278	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Page 16	Category 14 on page 16 is again too specific to metering systems and the "metering interface" should be made more generic where an example of that generic interface is a metering interface.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised the layout and example for logical interface category 14.	

Comment Number: 279	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 18	Comment	
	"However, the large legacy of devices in the field will need be addressed through mitigating technologies and methods." Should be changed to "However, the large number of legacy devices in the field will need use mitigating technologies and methods."	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 280	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 18	Comment	
	"Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists, and will require security controls (either physical or cryptographic) appropriate for wireless". This is a terrible sentence, so bad I can not even determine what it is trying to state and therefore can provide no suggestion.	
	Rationale/Recommendation	
	None	
	Disposition	

Comment Number: 280	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 281	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	There is a common statement in the document: "Some of the equipment is legacy (particularly the Remote Terminal Units (RTUs) which limit the types of security controls that could be implemented without replacing or upgrading the equipment" repeats a constraint already previously made and can be deleted - ie, an RTU is an IED ("IEDs can be limited in compute power, but that is becoming less of an ...").	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 282	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page 19	Comment	
	"Many of the SCADA Masters may have no way to add security without complete replacement". This is dangerously general and probably not true. There are products available today to secure SCADA communications and IEEE 1711 will be balloted soon, which provides a standard for these products to based upon.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 283	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 283	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Page 19	"No standard for security events or logging" is dangerously general and not true. IEEE 1686 provides logging standards for substation IEDs.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 284	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	I find it surprising that confidentiality of operations data is consistently given a low impact. Knowlegde of how the power system is operating can be leveraged by energy traders and be used to manipulate the energy market.	
	Rationale/Recommendation	
	None	
	Disposition	
	The focus in the second draft of the NISTIR is on power system reliability. Recognizing that certain critical information must be protected, there is a requirement to encrypt critical security parameters (CSPs), which may include operating information. Each organization will need to identify the CSPs that need to be encrypted.	

Comment Number: 285	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Category 8 is defined as "Sensor networks for measuring environmental parameters", which had me thinking this was simply addressing an analog transducer's connection to an IED for environmental data (like temperature), not a relay being used to measure current and voltage (since when are current and voltage environmental parameters?). The constraints given though make this sound like a collection of IEDs on a LAN, which would be the internal connections connections of a control system. This intent of this category needs to be clarified, because if it is truly the example as cited, then the contraints are not appropriate for that specific interface. Where this becomes even more	

Comment Number: 285	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	interesting is whether this category would include IEC 61850-9-2 process bus - a connection between a merging unit (sensor) and a relay (IED). Given that situation, some of the constraints are more appropriate for that interface. But a 61850-9-2 interface is completely different than a simple 0-1 VDC analog input signal.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 286	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Category 9 treats a substation master as a control system? This is an interesting choice of what a control system means. Defining a relay (or IED) as a sensor receiver is definitely interesting and not how the utility industry talks about relays and IEDs.	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR has revised logical interface category information.	

Comment Number: 287	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	"There is a typical statement made in the document: ""Data is typically time stamped at the source of measurement so that data from various devices can be correlated when analyzing system events. Modifying the internal clock or altering the time stamp in data exchanges may impact the utility's ability to determine the root cause of a system event."" This statement brings up modifying time stamps in data exchanges from only an operational standpoint (i.e. SCADA) but not protection. It has been discussed that differential protection using time-stamped measurements from two locations where one is an altered time stamp will cause an improper protective operation.	

<table>
<tr><td colspan="2">Comment Number: 287</td><td>Submitted by: IEEE</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5"></td><td colspan="3">Altering this time stamp is possible by altering the IRIG signal, but more importantly, through overriding the local GPS signal an altering the signal being sent to the satellite clock. Another example would be the use of synchrophasors to perform other operations. "</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">We will take this into consideration for the next version of the NISTIR.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 288</td><td>Submitted by: IEEE</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Page 30</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Discussion of category 13 is only concerned with wireless communications. Wired communications are not even discussed. This is a grave oversight. In addition, the criteria do not even mention access to the field devices for maintenance activities, but more connection back to the network and systems on that remote from the field system. Altering device configurations can make those devices operate improperly, and many of these devices support very limited forms of access control. This situation is not described in any category and is a grave oversight.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The second draft of the NISTIR has revised logical interface category information.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 289</td><td>Submitted by: IEEE</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="3">Reference:
3.5 – 3.11</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Sections 3.5-3.11 should really be under section 3.4 because they all relate to categorizations of each system interface to the 15 general cases in 3.4. This even makes a greater argument that the categories in section 3.4 require more abstraction that what presently exists.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
</table>

Comment Number: 289	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	None	
	Disposition	
	We will take this into consideration for the next version of the NISTIR.	

Comment Number: 290	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: 3.5 – 3.11	Comment	
	Sections 3.5-3.11 ignore remote access connections for device maintenance and configuration. This is a grave oversight.	
	Rationale/Recommendation	
	None	
	Disposition	
	Thank you for the comment, the drawings in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.	

Comment Number: 291	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: 3.5	Comment	
	Section 3.5 shows "RTUs or IEDs" inside one box while section 3.10 shows them in separate boxes. These should be shown exactly the same, not different, in order to properly capture all interfaces.	
	Rationale/Recommendation	
	None	
	Disposition	
	The diagrams in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.	

Comment Number: 292	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General

Reference: 3.10	Comment
	Section 3.10 shows no connection between the RTUs and IEDs. This interface can not be ignored.
	Rationale/Recommendation
	None
	Disposition
	The diagrams in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.

Comment Number: 293	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General

Reference: 3.10	Comment
	Section 3.10 shows no connection between the RTUs and PMU (which is an IED). This interface cannot be ignored. Note that some PMUs are actually relays, PMUs do not have to be dedicated devices independent of relays.
	Rationale/Recommendation
	None
	Disposition
	The diagrams in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.

Comment Number: 294	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General

Reference: 3.5 – 3.11	Comment
	Sections 3.5-3.11 do not properly show the "sensor network" as described in the categories. This results in section 3.10 completely disregarding these networks, which is incorrect.
	Rationale/Recommendation
	None
	Disposition

Comment Number: 294	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	The diagrams in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.	

Comment Number: 295	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: 3.10	Comment	
	Section 3.10 shows no PMU on the distribution system. Many relays offer embedded PMU capability and applications for the use of PMUs on the distribution system are being looked at. Not showing PMUs on the distribution system is an oversight. In effect, what is inside the transmission substation should also be shown inside the distribution substation.	
	Rationale/Recommendation	
	None	
	Disposition	
	Thank you for the comment, the drawings in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR. The diagrams in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.	

Comment Number: 296	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: 3.10	Comment	
	Section 3.10 does not show any interface in category 13. This has to be an oversight. Field crews regularly interface with substation IEDs, distribution IEDs, etc.	
	Rationale/Recommendation	
	None	
	Disposition	
	Thank you for the comment, the drawings and categories in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR. The diagrams in the second draft of the NISTIR have been updated and we will review for additional oversights in the next version of the NISTIR.	

Comment Number: 297	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.11	Comment	
	D.11 states that "A solution is needed to address the security and bandwidth constraints of this environment". This section needs to acknowledge the existence of IEEE 1711 which is going to ballot and will address the issue raised in D.11.	
	Rationale/Recommendation	
	None	
	Disposition	
	Noted, but this is not a final standard and is subject for review.	

Comment Number: 298	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.19	Comment	
	D.19 is titled outsourced WAN links but deals primarily with wireless issues and not enough with traditional circuit leasing from telcos. It is certainly not as interesting as wireless, but wired connections leased through telcos are at worst unsecured network clouds as well.	
	Rationale/Recommendation	
	None	
	Disposition	
	Great points. The Bottom Up group will consider how to accommodate these ideas in the next version of the NISTIR. Please consider joining the Bottom Up conference call and/or email suggestions to csctgbu@nist.gov to aid in developing specific text.	

Comment Number: 299	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.27	Comment	
	D.27 mentions the need for local authentication is required when connection to a centralized authentication server is lost. This would be similar to having a laptop and not being able to log on to it if there was no connection to the	

Comment Number: 299	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	corporate network and thus corporate authentication server. User accounts are cached on the laptop in order to facilitate logging on when no corporate network is present (and thus connection to corporate authentication server). It would be valuable to include this kind of discussion in D.20 to address whether or not this type of approach would work for the Smart Grid, provided additional features were also enabled, like logging and monitoring of what happens while not connected to the network. Is D.37 a repeat of D.27?	
	Rationale/Recommendation	
	None	
	Disposition	
	Great points. The Bottom Up group will consider how to accommodate these ideas in the next version of the NISTIR. Please consider joining the Bottom Up conference call and/or email suggestions to csctgbu@nist.gov to aid in developing specific text.	

Comment Number: 300	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.32	Comment	
	D.32 states that intrusion detection for DNP, Modbus, and 61850 need to be built for these systems. My understanding is that these already exist in vendor products for DNP and Modbus, perhaps not to the extent required, but at least started. One vendor is Industrial Defender.	
	Rationale/Recommendation	
	None	
	Disposition	
	We do not provide endorsements or reference to vendors; this document is vendor agnostic and is designed to provide requirements, not solutions.	

Comment Number: 301	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.39	Comment	
	D.39 should discuss what IEEE 1711 is doing to address the problem raised in this section.	

Comment Number: 301	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General

	Rationale/Recommendation
	None
	Disposition
	Noted, but this is not a final standard and is subject for review.

Comment Number: 302	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General

Reference: D.44	Comment
	D.44 should discuss what IEEE 1711 is doing to address the problem raised in this section, and this section may be a repeat of D.11 and/or D.12.
	Rationale/Recommendation
	None
	Disposition
	Noted, but this is not a final standard and is subject for review.

Comment Number: 303	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General

Reference: 3.3	Comment
	"""Wireless media is often less expensive than wired media, which mean that wireless vulnerabilities exists"" - What is the correlation between media costs and vulnerabilities? Why is the fact that wireless media is less expensive an indicator for vulnerabilities?"
	Rationale/Recommendation
	None
	Disposition
	The intent is not to correlate that wireless means cheap and that cheap is vulnerable; it is attempting to indicate that the use of wireless increases the threat surface of the Smart Grid.

Comment Number: 304	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: 3.3 (Page 18)	Comment	
	"IEDs can be on pole tops and other insecure locations". This should refer to physical insecure locations.	
	Rationale/Recommendation	
	"IEDs may be located on pole tops and other locations with limited physical security"	
	Disposition	
	Good point. We will be taking this into consideration for the next version of the NISTIR.	

Comment Number: 305	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page A-22	Comment	
	Potential Stakeholder Issues • Customer safety • Device standards • Cyber Security What is meant by Cyber Security as a potential issue? Isn't this the overall goal here?"	
	Rationale/Recommendation	
	Remove Cyber Security from list of issues	
	Disposition	
	The Use Cases represent a business case and in that respect are evaluated in terms of what the stakeholder concerns are. We will re-evaluate this section for the next draft of the NISTIR.	

Comment Number: 306	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page A-22	Comment	
	Potential Stakeholder Issues • Customer safety • Device standards	

Comment Number: 306	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	• Cyber Security All other Distribution Automation Use cases list Customer Device Standards as an issue.	
	Rationale/Recommendation	
	Change "Device Standards" to Customer Device Standards to be consistent	
	Disposition	
	Noted. We will change the wording to be consistent in the next version of the NISTIR.	

Comment Number: 307	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page A-29, A-36, A-38	Comment	
	"""Potential Stakeholder Issues - Cyber Security"" Isn't Cyber Security the overall goal and could be added to all use cases as an issue also?"	
	Rationale/Recommendation	
	Either remove Cyber Security as a stakeholder issue from all use cases or add it to all.	
	Disposition	
	The Use Cases represent a business case and in that respect are evaluated in terms of what the stakeholder concerns are. We will re-evaluate this section for the next draft of the NISTIR.	

Comment Number: 308	Submitted by: IEEE	Comment Type: __ Technical _X_ Editorial __ General
Reference: C.2.1 (Page C1)	Comment	
	Change title	
	Rationale/Recommendation	
	C.2.1 Personnel	
	Disposition	

Comment Number: 308	Submitted by: IEEE	Comment Type: __ Technical _X_ Editorial __ General
	Please re-submit your question. We are not sure what you are asking.	

Comment Number: 309	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: C.2.2.1 (Page C-2)	Comment	
	Move C.2.2.1 under C.2.1	
	Rationale/Recommendation	
	None	
	Disposition	
	Consensus was to leave the organization as it currently exists.	

Comment Number: 310	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: C.3.1.1 (Page C-6)	Comment	
	C.3.1.1 list "Poor Logging Practice" as an example, which is also listed under C.3.1.9	
	Rationale/Recommendation	
	Remove "Poor Logging Practice" from C.3.1.1	
	Disposition	
	Consensus was to leave the organization as it currently exists.	

Comment Number: 311	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: Page C-16	Comment	
	Buffer Overflow is listed a separate vulnerability class but also listed several times as example for other classes. This might be confusing.	
	Rationale/Recommendation	

Comment Number: 311	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
	None	
	Disposition	
	Consensus was to leave the organization as it currently exists.	

Comment Number: 312	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.32 (Page D-11)	Comment	
	Talks about IDS. The same applies for firewalls and IPS.	
	Rationale/Recommendation	
	None	
	Disposition	
	Noted. This will be addressed in the next revision of the NISTIR.	

Comment Number: 313	Submitted by: IEEE	Comment Type: _X_ Technical __ Editorial __ General
Reference: D.49 (Page D-15)	Comment	
	IEC TC57WG15 (IEC 62351) is looking into RBAC with one aspect being the set of roles needed.	
	Rationale/Recommendation	
	None	
	Disposition	
	IEC 62351 will be reviewed when it is final.	

Comment Number: 314	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section1.3	Comment	
	Smart Grid Cyber Security is more than just communications security (COMSEC). The definition of Cyber	

Comment Number: 314	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General
	Security is presently too focused on just communications infrastructure. Section 1.3 shows the definition of Cyber Infrastructure and of Cyber Security, but these are inconsistent as written. Cyber Security should be defined throughout this document as "Cyber Security: the protection required to ensure confidentiality, integrity and availability of the Smart Grid Cyber Infrastructure, including the control systems, sensors and actuators." The point is to protect the entire Cyber Infrastructure, not just the communications links. There is significant discussion in legislation and policy about the threats against which the 'Smart Grid' must be protected, yet the draft NISTIR document gives no guidance on this.	
	Rationale/Recommendation	
	Recommend revising Section 1.3 (Scope, Risks and Definitions) to include reference to Table 4.1 of the Information Assurance Technical Framework, and to give guidance as to which adversary sets (from Script Kiddies to Nation State Adversaries) various grid control systems must protect against. See http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA393328&Location=U2&doc=GetTRDoc.pdf	
	Disposition	
	We have revised the definition of cyber security to be more inclusive of the IT, Telecommunications, and electric sectors. We will consider this comment for the next version of the NISTIR.	

Comment Number: 315	Submitted by: Boeing	Comment Type: _X Technical _ Editorial __ General
Reference: Section 1.4 Page 3	Comment	
	Reference text: "The protection required to ensure confidentiality, integrity and availability of the electronic information communication system"	
	Rationale/Recommendation	
	Change text to read: "The protection required to ensure confidentiality, integrity and availability of the Smart Grid Cyber Infrastructure, including the control systems, sensors and actuators."	
	Disposition	
	The definition has been revised to address this comment.	

Comment Number: 316	Submitted by: Boeing	Comment Type: _X_ Technical Editorial __ General
Reference:	Comment	

Comment Number: 316	Submitted by: Boeing	Comment Type: _X_ Technical Editorial __ General

Chapter 4 Page 56	Delete “AMI” from section title Note – This is related to adding a section on “Smart Grid Control Systems Security Requirements” to this section.
	Rationale/Recommendation
	Change Section Title to: “Security Requirements”
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 317	Submitted by: Boeing	Comment Type: __ Technical _X_ Editorial __ General

Reference: Chapter 4 Page 56	Comment
	Note – This is related to adding a section on “Smart Grid Control Systems Security Requirements” to this section.
	Rationale/Recommendation
	Change the first paragraph of the section to read: “The security requirements in Section 4.1 were developed by ASAP-SG. They are included in the document Security Profile for Advanced Metering Infrastructure, Version 0.44, September 17, 2009. This document was published by the ASAP-SG for the UtiliSec Working Group (UCAIug) and the NIST Cyber Security Coordination Task Group. The AMI requirements have been included here with permission of the ASAP-SG. The security requirements in Section 4.1 are modeled substantially after the same work by the ASAP-SG. However, they have been modified as appropriate to Non-AMI Smart Grid Control Systems.”
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 318	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General

<table>
<tr><td>Comment Number: 318</td><td colspan="2">Submitted by: Boeing</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Chapter 4
Page 56</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Add text.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Add the following to the end of the section 4 intro: “It is recognized that the Federal Energy Regulatory Commission (FERC) has regulatory authority over many aspects of the electric utility industry. Should there be a conflict between the requirements presented here and the requirements presented in separate documents issued under FERC authority, the requirements in the FERC documents will govern.”</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">This comment will be considered for the next version of the NISTIR.</td></tr>
</table>

<table>
<tr><td>Comment Number: 319</td><td colspan="2">Submitted by: Boeing</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference:
Section 4</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Add section addressing “Smart Grid Control System Security Requirements”</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3"><b>4.2 Smart Grid Control System Recommended Requirements</b>
This section closely parallels Section 4.1 above. The requirements, however, have been changed as appropriate to the non-AMI related intelligent components (sensors, actuators, systems) of the Smart Grid Control Systems. The following requirements are adapted from the DHS Catalog of Control Systems Security[4] and have been modified or extended as appropriate for Smart Grid Control System security. The DHS requirement section numbers are only provided for traceability, and not intended to indicate that the requirements in this document are the DHS requirements themselves. When the ASAP-SG team created requirements for which there was no DHS counterpart, the "ASAP-" prefix is used instead of "DHS-". For each requirement, the NIST SP 800-53 reference is included.</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">The second draft of the NISTIR includes requirements for the entire Smart Grid. We will consider this comment</td></tr>
</table>

[4] Department of Homeland Security, National Cyber Security Division. January 2008. Catalog of Control Systems Security: Recommendations for Standards Developers. Retrieved from http://www.us-cert.gov/control_systems/

Comment Number: 319	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General
	for the next version of the NISTIR.	

Comment Number: 320	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General

Reference: Overall	Comment
	Add section for SGIP-CSWG control system criticality model.
	Rationale/Recommendation

SGIP-CSWG Multi-Tier Control System Criticality Model

Using a similar architecture (deleted as is) (inserted to that) used in high assurance control systems is appropriate to many Smart Grid Control Systems. This model expands beyond binary Critical/Non-Critical assessments to allow four levels of criticality in Smart Grid Control Systems. These levels are determined based on the impact of failure of the component or system being assessed. In the future FERC may release different objective criteria for defining the levels of impact. If/when that happens, the definitions here will be superseded by the FERC definitions.

These definitions are intended to provide an objective measure of impact when viewed from a national perspective. They also provide a mechanism whereby small utilities, such as small municipal utilities and rural electric cooperatives, are not impacted with the same burden of protective controls as would be appropriate to large urban/regional utilities. Any operating company may implement more stringent criteria, but may not implement less stringent criteria.

Levels of Impact of failure are as follows:

1. Catastrophic – more than 1,000,000 customers impacted
2. High – 100,000 to 1,000,000 customers impacted
3. Medium – 1,000 to 100,000 customers impacted
4. Low – Fewer than 1,000 customers impacted

When determining impact of failure, consideration must be given to the potential for cascading failures. In order for systems to be assessed as having the potential for anything less than Catastrophic Impact, there must be sufficient fault isolation capabilities in the system to prevent lower-impact failures from cascading further into the Grid. For

Comment Number: 320	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General

example, Medium Impact systems may be detrimentally impacted by adjacent High Impact system failures, but High Impact systems must not be caused to fail by adjacent Medium Impact system failures.

Failure of at least two actuators or Transmission Feeders must be assumed when planning outage prevention for Catastrophic Impact systems.

Failure of at least two actuators or one Transmission Feeder or two Distribution Feeders must be assumed when planning outage prevention for High Impact system.

Disposition

This comment is being reviewed for inclusion in the next version of the NISTIR.

Comment Number: 321	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General

Reference: Overall

Comment

Add section for SGIP-CSWG Smart Grid control system trust model.

Rationale/Recommendation

SGIP-CSWG Smart Grid Control System Trust Model

While it is anticipated that all best practices for IT security will be followed for Smart Grid systems, engineering for fault tolerance is still required. Field actuators with Catastrophic or High Impact of failure must be engineered to perform their function properly even if any one of its sensor or command inputs is compromised through error or active attack. This is referred to as Adjacent Subsystem Mutual Distrust.

No system or actuator with High or Catastrophic impact of failure may take action based on a single (potentially erroneous or compromised) command input. All such actuators must limit their susceptibility to single-source failure, compromise or attack by having a secure method of synthesizing inputs from a combination of local and distributed sensors, and control room or control center commands.

Disposition

Comment Number: 321	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General
	This comment is being reviewed for inclusion in the next version of the NISTIR.	

Comment Number: 322	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Add a section for SGIP-CSWG threat-based requirements.	
	Rationale/Recommendation	

SGIP-CSWG Threat-based Requirements

Several categories of threats to Critical Infrastructure are recognized by the Federal Government. Those applicable to the Smart Grid are described briefly in the table below.

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, which is normally not very well organized or financed. Normally consists of very few individuals, or of one individual acting alone.

Comment Number: 322	Submitted by: Boeing	Comment Type: _X_ Technical __ Editorial __ General

Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or Poorly Trained Employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another example of an insider threat or adversary.

Source: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA393328&Location=U2&doc=GetTRDoc.pdf .

Smart Grid systems and actuators which have the potential for Catastrophic or High Impact when they fail must protect against all of the listed threat categories.

Disposition

This comment is being reviewed for inclusion in the next version of the NISTIR.

Comment Number: 323	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 2

Comment

NIST should establish comprehensive privacy regulations that limit the collection and use of consumer data.

Rationale/Recommendation

None

Disposition

Several valid points raised by privacy comments were important; however, they fell outside the scope of our work. Also regulations are outside the scope of the SGIP-CSWG.

Comment Number: 324	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 2	Comment
	NIST’s Cyber Security Strategy report properly recognizes that one of the risks posed by the Smart Grid is the “[p]otential for compromise of data confidentiality, include the breach of customer privacy.” Within the rubric of potential risks to customer privacy, NIST conducted a Privacy Impact Assessment, examining the “privacy implications and related information security safeguards within the planned U.S. Smart Grid, particularly issues involved with consumer-to-utility data items collected and how they are used.” NIST concluded that “[t]he results of a high-level PIA of the consumer-to-utility metering data sharing portion of the Smart Grid reveal that significant areas of concern must be addressed within each localized region of the Smart Grid.”More specifically, NIST found that the “lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed.” NIST then identified ten principles “as a starting point for the development of appropriate protections for PII collected and/or used within the Smart Grid.” However, several of the principles are flawed, and NIST relies too heavily on the discredited notice and consent model of privacy protection. This comment proposes ways to strengthen NIST’s recommendations for privacy protection in the Smart Grid environment.
	Rationale/Recommendation
	NIST’s approach to Smart Grid privacy is insufficient.
	Disposition
	The privacy chapter has been significantly revised and includes privacy practices.

Comment Number: 325	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 2	Comment
	PII activity should, as mentioned, be limited to a permitted and specified purpose. EPIC agrees that “only the minimum amount of data necessary for the utility companies to use for energy management and billing should be collected.” EPIC also agrees that treatment of information must conform to fair information practices. However, NIST should specify that those practices match the practices identified in the HEW Report and the OECD Privacy Guidelines. As discussed, the HEW Report established fair information practices, based on five principles: (1) There

<table>
<tr><td>Comment Number: 325</td><td>Submitted by: EPIC</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5"></td><td colspan="2">must be no personal data record---keeping systems whose very existence is secret. (2) There must be a way for a person to find out what information about the person is in a record and how it is used. (3) There must e a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without he person's consent. (4) Here must be a way for a person of correct are amend a record of identifiable information about the person. (5) Any organization creating, maintaining, using, or disseminating records Of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.
Similarly, the OECD Privacy Guidelines established eight principles for data legislation: Collection Limitation; Data Quality; Purpose Specification; Use Limitiation; Security Safegauards; Opennes; Individual Participation; and Accountability. The treatment of Smart Grid information should conform to those practices</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">Adopt fair information practices.</td></tr>
<tr><td colspan="2">Disposition</td></tr>
<tr><td colspan="2">The second draft of the NISTIR 7628 has a rewritten privacy chapter with privacy practices that address many of these concerns.</td></tr>
</table>

<table>
<tr><td>Comment Number: 326</td><td>Submitted by: EPIC</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5">Reference: Chapter 2</td><td colspan="2">Comment</td></tr>
<tr><td colspan="2">Moreover, NIST should require enforcement of the guidelines in accordance with the HEW Report. NIST should recommend enforcement mechanisms, such as civil and criminal penalties, injunctions and private rights of action. By specifying the parameters and enforcement of the fair information practices, NIST can require actual conformance, rather than loosely requiring treatment to “conform.”</td></tr>
<tr><td colspan="2">Rationale/Recommendation</td></tr>
<tr><td colspan="2">Adopt fair information practices.</td></tr>
<tr><td colspan="2">Disposition</td></tr>
</table>

Comment Number: 326	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General
	The second draft of the NISTIR 7628 has a rewritten privacy chapter. .Enforcement is outside the scope of the SGIP-CSWG.	

Comment Number: 327	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 2	Comment
	NIST proposes that "[d]ocumented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors and other entities with management responsibilities throughout the Smart Grid should be created implemented, and compliance enforced." However, it may be insufficient for organizations to simply provide privacy training to their employees or even to appoint dedicated privacy officers with audit functions. For example, in an analogous situation, despite the training and audit authority conferred to the Chief Privacy Office of the Department of Homeland Security, that office has proven to be impotent, powerless to effectively protect Privacy. On a range of issues, from whole body imaging to suspicion less electronic border searches, the Chief Privacy Officer for DHS has failed to fulfill her statutory obligations. Accordingly, EPIC and other privacy and civil liberties groups have called or Congress to consider the establishment of alternative oversight mechanisms, including the creation of an independent office. Without such an independent office, it would be impossible to ensure the proper Smart Grid Standards protection of privacy rights, because the decisions of the Chief Privacy Officer would continue to be subject to the oversight of the Secretary and the rest of the executive branch. Similarly, for Smart Grid organizations to appoint privacy personnel or simply train existing personnel would be an ineffective solution that would only serve to preclude the possibility of creating an independent position with actual authority to protect privacy.
	Rationale/Recommendation
	Establish independent privacy oversight - NIST should recommend that an independent Privacy Office, with completely independent authority be established, with power over all entities associated with the Smart Grid.
	Disposition
	Establishing privacy training and awareness activities is not unique to the Smart Grid and many utilities have already established this based on the security requirements for training and awareness. Several points in this comment are outside the scope of the SGIP-CSWG..

Comment Number: 328	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 328	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 2	Comment
	The NIST principles rely heavily on the notice and consent model: “A clearly-specified notice should exist to describe the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection. . . . The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of their PII. As a threshold matter, the purposes for which PII can be collected, used, retained, or shared should be severely restricted. The purposes for which PII can be collected, used, retained, or shared should be severely restricted. It is insufficient to simply require authorities or organizations to have a nebulous “purpose,” as anything from “improved marketing” to “government surveillance” could qualify.
	Rationale/Recommendation
	Abandon the Notice and Consent model. NIST should recommend that a formal rulemaking be established so that service providers establish a concrete set of approved purposes for which PII activity is permitted. That list of approved purposes should be very limited, and only purposes essential to the functioning of the Smart Grid should be permitted.
	Disposition
	The second draft of the NISTIR includes a significantly revised privacy chapter that includes privacy practices that address these comments.

Comment Number: 329	Submitted by: EPIC	Comment Type: __x Technical __ Editorial __ General

Reference: Chapter 2	Comment
	The NIST guidelines propose that:” Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it. . . .PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.” It is insufficient to simply say that information should be used or disclosed only for a permitted purpose. Instead, NIST must require organizations to follow those policies, and must provide the authorities with the power to enforce them. Furthermore, it is inadequate to permit PII to be retained “as long as is necessary to fulfill the purposes for which it was collected.” That standard is entirely too lenient, and it would permit organizations too much leeway to retain information whenever they deem it necessary. Instead, NIST should set expiration dates on PII so that PII can be

Comment Number: 329	Submitted by: EPIC	Comment Type: __x Technical __ Editorial __ General
	retained only for a certain period of time.99 The length of time could vary based on the type of PII and the purpose for which it was collected. A concrete expiration date would make the system more transparent for consumers, as they would be more aware of the lifespan of their data.	
	Rationale/Recommendation	
	NIST must ensure that restrictions on the use and retention of data are mandatory, not inspirational.	
	Disposition	
	The second draft of the NISTIR includes a significantly revised privacy chapter that includes privacy practices that address these comments.	

Comment Number: 330	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	NIST has done significant work on the topic of role--based access control to computer records and systems. In this context, role--based access control protocols should strictly manage when, where, who and how PII in Smart Grid data is accessed. Access to PII, including electricity usage, should be limited to the function of the position an individual fills within the Smart Grid service delivery and billing relationship. Graduated levels of access should be based on responsibilities for providing Smart Grid FIPs and service provision purposes. Access should be monitored by log files and auditing of access use and resolution of issues related to customer service and proper operation of the Smart Grid.	
	Rationale/Recommendation	
	NIST should implement role-based access control to Smart Grid data.	
	Disposition	
	The second draft of the NISTIR in Appendix D 4.25 has been revised and we will review and consider this comment for the next version of the NISTIR.	

Comment Number: 331	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 2	Comment	
	As discussed, the Supreme Court in Kyllo v. United States addressed the interaction between the Fourth	

Comment Number: 331	Submitted by: EPIC	Comment Type: _X_ Technical __ Editorial __ General
	Amendment and the monitoring of electrical use, holding that the police could not use thermal imaging equipment, which was not in general public use, “to explore details of the home that would previously have been unknowable without physical intrusion,” without first obtaining a search warrant. As the Court recognized, “’At the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’” Similarly, in the Smart Grid context, NIST should make clear that the Fourth Amendment protects the information of Smart Grid consumers, and that law enforcement must first obtain a Search warrant before gaining access to the information.	
	Rationale/Recommendation	
	NIST should explicitly address law enforcement access to Smart Grid data and should ensure that their access complies with the strictures of the Fourth Amendment.	
	Disposition	
	Several points in this comment are outside the scope of the SGIP-CSWG.	

Comment Number: 332	Submitted by: AT&T	Comment Type: __ Technical __ Editorial _X_ General
Reference: Overall	Comment	
	AT&T encourages NIST to assure there is consistency and clarity of meaning for terms used within the document. For example, the term "organization" is repeatedly used. AT&T understands this term to mean the electric utility operator that is ultimately responsible for the security measures. Likewise, care should be exercised to assure that terms like "vendor", "supplier", and "commercial service provider" have clear and consistent meaning and use throughout the revised Cyber Security Requirements.	
	Rationale/Recommendation	
	A definitional section at the beginning of the report would help to avoid any confusion or misinterpretation of these terms.	
	Disposition	
	We have included a glossary in the second draft of the NISTIR. We will consider this comment as we develop the next version of the NISTIR.	

Comment Number: 333	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 2.5.2	Comment
	Reference text: “The new smart meters and accompanying potential and actual uses create the need for utilities to be more transparent and clearly provide notice documenting the types of information items collected, and the purposes for collecting the data. Within the Smart Grid implementation a clearly-specified notice must describe the purpose for the collection, use, retention, and sharing of PII. Data subjects should be told this information at or before the time of collection.”
	Rationale/Recommendation
	The party to receive notice should be clarified. in the case of individual homes or units, the customer will receive the notice. However, clarification is needed in the case of multi-tenant and multi-dwelling units. in many cases, the building manager will manage the utility meters for the tenants. Clarification is needed regarding who is the customer, to whom notice should be given, etc. in the multi-tenant environment, there are complexities regarding protection of privacy and communication of privacy related information. Revise this section as follows: “The new smart meters and accompanying potential and actual uses create the need for utilities to be more transparent and clearly provide notice documenting the types of information items collected, and the purposes for collecting the data. Within the Smart Grid implementation a clearly-specified notice must describe the purpose for the collection, use, retention, and sharing of PII. Data subjects, including the customer and any building manager with the customer's consent, should be told this information at or before the time of collection.”
	Disposition
	We know that this is an identified risk, and we have been addressing multiple dwelling units (MDUs), as we talk about renters and lessors. We have included privacy practices in the second draft of the NISTIR that address disclosure issues.

Comment Number: 334	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 2.5.3	Comment
	Reference text: “New smart meters create the need for utilities to give residents a choice about the types of data collected. Utilities should obtain consent from residents for using the collected data for other purposes, and as a requirement before data can be shared with other entities. Clearly there should be meaningful informed consent in the instances where information is collected for use for marketing or advertising purposes. However, other information

<table>
<tr><td>Comment Number: 334</td><td colspan="2">Submitted by: AT&T</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="5"></td><td colspan="3">may be necessary for planning, engineering and management of the communications infrastructure. Consent should not be required in this case to use data, including ph for these purposes. Access to information for such purposes should be identified as an exception not covered by customer choice and consent for information use.”</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Revise this section as follows: “New smart meters create the need for utilities to give residents a choice about the types of data collected. Utilities should obtain customer consent where information is collected for use for marketing or advertising purposes. However, such consent is not required for the collection, use, retention, and sharing of PII for the purposes necessary for planning, engineering and management of the communications network and infrastructure supporting the Smart Grid. Utilities should obtain consent from residents for using the collected data for other purposes, and as a requirement before data can be shared with other entities.”</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">We have included privacy practices in the second draft of the NISTIR that address consent issues.</td></tr>
</table>

<table>
<tr><td>Comment Number: 335</td><td colspan="2">Submitted by: AT&T</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="4">Reference: Section 2.5.4</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">Reference text: “In the current operation of the electric grid, data taken from meters consists of basic data usage readings required to create bills. Under a Smart Grid implementation, meters and will collect other types of data. Some of this additional data may be PII. Because of the associated privacy risks, only the minimum amount of data necessary for the utility companies to use for energy management and billing should be collected. However, the amount of information collected may vary, depending on whether or not power generation occurs on the premises. Home generation services will likely increase the amount of information created and shared.“

Disclosures should describe the type of information collected in a reasonably detailed manner. Mechanisms are needed to adapt the disclosures and reaffirm consent when the nature of the information collected is changed in a material manner. Requirements should include provisions to address permissible use of information. For example as discussed in section 2.5.3, or when the PII information is aggregated and anonymity is provided.”</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">Insert the following text at the end of this section: “Disclosures of data collection should describe the type of information collected in a reasonably detailed manner. Should the type of data collected, used, retained and/or shared,</td></tr>
</table>

Comment Number: 335	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	including PII change, an updated disclosure should be sent to the customer and/or building manager. The second sentence of the original text appears to have a typographical error and should be corrected as suggested below: "Under a Smart Grid implementation, meters will collect other types of data."	
	Disposition	
	We have included privacy practices in the second draft of the NISTIR that address disclosure issues.	

Comment Number: 336	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 2.5.5	Comment	
	Reference text: "In the current operation of the electric grid, data taken from meters is used to create residents' bills, determine energy use trends, and allow customers to control their energy usage both on-site and remotely. The new smart meters, and the Smart Grid network, will have the capability to use the collected data in an unlimited number of ways. Information should only be used or disclosed for the purpose for which it was collected; and should be divulged only to those parties authorized to receive it. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. PII should only be kept as long as is necessary to fulfill the purposes for which it was collected." The specific length of PII data retention should be discussed. Each utility should have its own retention records guidelines. Retention guidelines should be established by each utility when data is retained in the aggregate and with specific anonymity that will be used to protect customers' privacy when data is maintained and retained for other purposes.	
	Rationale/Recommendation	
	Insert the following text at the end of this section: Each utility should establish its own retention guidelines for the retention of data collected. Additionally, specific anonymization and aggregation strategies should be established by each utility when such data is retained for other purposes.	
	Disposition	
	We have included privacy practices in the second draft of the NISTIR that address these issues.	

Comment Number: 337	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.2.1	Comment	
	Reference: “AMI components must separate telemetry/data acquisition services from management port functionality. “	
	Rationale/Recommendation	
	ALTHOUGH SEPARATION IS APPROPRIATE, THIS SECTION SHOULD CLARIFY THAT THERE IS NO REQUIREMENT FOR PHYSICAL SEPARATION. Revise this section as follows: “AMI components must separate telemetry/data acquisition services from management port functionality through reasonable virtual or physical segregation strategies.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 338	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.4.1	Comment	
	Reference: “AMI components shall prevent unauthorized or unintended information transfer via shared system resources. “	
	Rationale/Recommendation	
	THE REQUIREMENT SHOULD NOT BE LIMITED TO SHARED RESOURCES. Revise this section as follows: “AMI components shall prevent unauthorized or unintended information transfer.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document	

Comment Number: 338	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 339	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.5.1	Comment	
	Reference: "AMI components shall protect against or limit the effects of denial-of-service attacks. "	
	Rationale/Recommendation	
	RATHER THAN ALL INDIVIDUAL COMPONENTS PROVIDING DEFENSE AGAINST DENIAL OF SERVICE, THE AMI ARCHITECTURE SHOULD BUILD IN CAPABILITIES THAT DEFEND AGAINST INDIVIDUAL METERS BEING COMPROMISED AND, SHOULD THAT OCCUR, THAT STEPS CAN BE TAKEN TO ISOLATE THE BREACH. Insert the following text at the end of this section: "The AMI architecture shall include capabilities that provide monitoring and defensive measures that afford early detection of denial-of-service attacks and enable steps to be taken that limit the impact."	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 340	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.6.1	Comment	
	Reference: "AMI components must limit the use of resources by priority."	
	Rationale/Recommendation	
	CLARIFICATION SHOULD BE CONSIDERED WITH RESPECT TO THE PURPOSE OF THIS REQUIREMENT. Insert the following text at the end of this section: "The design of the AMI platform shall include provisions that	

Comment Number: 340	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	reasonably assure security measures are not adversely impacted by AMI transaction volume.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 341	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.7.1	Comment	
	Reference: “The organization shall define the external boundary(ies) of the AMI system. Procedural and policy security functions must define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The AMI system monitors and manages communications at the operational system boundary and at key internal boundaries within the system. In AMI, the very concept of boundaries is problematic. Internal systems within the organization may be more easily protected than components which reside outside significant physical boundaries and controls.”	
	Rationale/Recommendation	
	THE TERM “OPERATIONAL SYSTEM BOUNDARY” AND THE GENERAL TERM “BOUNDARY(IES)” ARE NOT DEFINED. Revise this section as follows: “The organization shall define the external boundary(ies) of the AMI system. Procedural and policy security functions must define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The AMI system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.-The organization shall define the required strength of security measures and the level of barriers to unauthorized access and control of system assets at all external system boundary(ies) and at critical internal system boundary(ies). A boundary is this context means any physical or logical interface to a networking or management subsystem to the extent the functionality is directly supporting Smart Grid operation for a particular utility.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in	

Comment Number: 341	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

	the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 342	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.8.8.1	Comment
	Reference: “The AMI system design and implementation must protect the integrity of electronically communicated information. “
	Rationale/Recommendation
	THE PROTECTION SHOULD BE APPLIED TO THE NETWORK AND THE APPLICATION LAYER. Revise this section as follows: “The AMI system application layer design and implementation must include features that protect the integrity of electronically communicated information. “
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 343	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.8.9.1	Comment
	Reference: “The AMI system design and implementation must protect the confidentiality of communicated information where necessary. “
	Rationale/Recommendation
	VARYING LEVELS OF PROTECTION ARE APPROPRIATE REFLECTING THE NATURE OF THE COMMUNICATIONS AND THE VALUE/RISK IMPLICIT IN UNAUTHORIZED ACCESS.

Comment Number: 343	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	Revise this section as follows: " The AMI system design and implementation must protect the confidentiality of communicated information commensurate with the value of the information and the risk of harm resulting from unauthorized access."	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 344	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.10.1	Comment	
	Reference: "The AMI system must establish trusted communications paths between the user (or agent) and the components making up the AMI system. "	
	Rationale/Recommendation	
	THE PATH IS ONLY ONE PART OF THE ENTIRE CONNECTION AND THE PATH ITSELF MAY BE VIRTUAL OR PHYSICAL. Revise this section as follows: "The AMI system must establish and support trusted communications ~~paths~~ exchanges between the user (or agent) and the components making up the AMI system. "	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 345	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 345	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Chapter 4 DHS-2.16.3.1	Reference: "All AMI components must capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes. "	
	Rationale/Recommendation	
	SERVICE PROVIDERS SHOULD HAVE PROCEDURES TO CAPTURE DETAILED AUDIT RECORDS AND OTHER INFORMATION IN THEIR NETWORK. Insert the following text at the end of this section: "All AMI components under the direct control of the organization must capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes. Commercial service providers delivering AMI components shall document and follow and periodically internally audit compliance with procedures designed to capture equivalent information for communications capabilities supplied as part of the AMI system. "	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 346	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.11.1	Comment	
	Reference: "When cryptography is required and employed within the AMI system, the organization shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. "	
	Rationale/Recommendation	
	CLARIFICATION SHOULD BE CONSIDERED SUCH THAT THE ORGANIZATION CAN USE A THIRD PARTY TO ESTABLISH AND MANAGE KEYS. Revise this section as follows: "When cryptography is required and employed within the AMI system, the organization is responsible to assure that cryptographic keys are-managed using automated mechanisms with supporting manual procedures should the automated mechanisms fail.	
	Disposition	

Comment Number: 346	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 347	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.12.1	Comment	
	Reference: “The organization shall develop and implement a policy governing the use of cryptographic mechanisms for the protection of AMI system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance. “	
	Rationale/Recommendation	
	NIST SHOULD TAKE STEPS TO CERTIFY ALGORITHMS FOR SMALLER INTELLIGENT ELECTRONIC DEVICES (“IEDS”) WITH PROCESSORS THAT HAVE LIMITED COMPUTING POWER AND ARE NOT CAPABLE OF SUPPORTING ADVANCED ENCRYPTION STANDARD (“AES”). Revise this section as follows: “The organization shall develop and implement a policy governing the use of cryptographic mechanisms and tailored to the processing power of the using devices to protect AMI system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance. “	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 348	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	Reference: “The use of collaborative computing mechanisms on AMI components is strongly discouraged and	

Comment Number: 348	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
DHS-2.8.13.1	provides an explicit indication of use to the local users. Alternative statement: Given the current state of this technology and/or the ability to secure it would substantially increase the security risk at this time. “	
	Rationale/Recommendation	
	THIS REQUIREMENT COULD BE MISCONSTRUED TO PROHIBIT JOINT USE OF COMMERCIAL NETWORKS. . Revise this section as follows: “Collaborative computing mechanisms on AMI components may be used provided security is assured. Although the organization may opt to prohibit individual collaborative computing mechanisms on its AMI platform, this limitation does not apply to commercial service providers nor does it prevent use of a commercial service provider that can safeguard AMI transactions that it handles.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 349	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.17.1	Comment	
	Reference: “The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and limits the use of VOIP within the AMI system. Given the current state of this technology and/or the ability to secure it would substantially increase the security risk at this time. “	
	Rationale/Recommendation	
	THE ORGANIZATION SHOULD HAVE THE OPTION TO RESTRICT THE NATURE OF THE SERVICES SUPPORTED ON THE INFRASTRUCTURE THAT IT OWNS AND DIRECTLY CONTROLS. HOWEVER, CLARIFICATION OF THIS REQUIREMENT SHOULD BE CONSIDERED TO NOT FORECLOSE THE USE OF COMMERCIAL CARRIER NETWORKS THAT CAN ASSURE VIRTUAL SEGREGATION OF TRAFFIC WHEN	

Comment Number: 349	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

	PHYSICAL NETWORK RESOURCES ARE ACCESSED BY MULTIPLE USERS. Insert the following text at the end of this section: “An organization’s choice to limit the use of VoIP on the AMI Infrastructure does not apply to commercial service providers, nor does it prevent use of a commercial service provider that can safeguard AMI transactions it handles.”
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 350	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.8.18.1	Comment
	Reference: “All external AMI components and communication connections must be identified and adequately protected from tampering or damage. “
	Rationale/Recommendation
	THIS REQUIREMENT COULD BE INTERPRETED TO PLACE EACH COMPONENT IN A COMMERCIAL NETWORK UNDER THE REVIEW AND CERTIFICATION OF THE UTILITY. COMMERCIAL NETWORKS ALREADY FOLLOW INTERNATIONAL BEST PRACTICES AND MEET FEDERAL GOERNMENT REQUIREMENTS IN THIS AREA. Insert the following text at the end of this section: “The organization shall assure external AMI components and communication connections are identified and adequately protected from tampering or damage. Any protective measures beyond those already applied by a commercial service provider that the organization seeks to augment shall be set forth in a contractual agreement between the organization and the commercial service provider.”
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG

Comment Number: 350	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	Security WG for disposition.	

Comment Number: 351	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.8.20.1	Comment	
	Reference: “The AMI system must provide mechanisms to protect the authenticity of device-to-device communications.”	
	Rationale/Recommendation	
	AUTHENTICATION AND INTEGRITY OF AMI DEVICE-TO-DEVICE COMMUNICATION SHOULD BE PERFORMED AT THE APPLICATION LAYER. Revise this section as follows: “The AMI system must provide mechanisms to protect the authenticity of device-to-device communications at the application layer.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 352	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.9.1.1	Comment	
	Reference: “The organization shall develop, disseminate, and periodically review/update: 1. A formal, documented, AMI system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. 2. Formal, documented procedures to facilitate the implementation of the AMI system information and document	

Comment Number: 352	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

	management policy and associated system maintenance controls. “
	Rationale/Recommendation
	CLARIFICATION SHOULD BE CONSIDERED TO CLARIFY THAT THE ORGANIZATION (UTILITY) IS RESPONSIBLE FOR MEETING THESE OBLIGATIONS. TO THE EXTENT THAT SUPPLIERS CONTRIBUTE TO FULFILLING THEIR RESPONSIBILITIES, THEN UTILITIES SHOULD ENTER INTO A CONTRACTUAL AGREEMENT WITH THE SUPPLIER THAT WILL ENABLE THE UTILITY TO MEET THESE REQUIREMENTS. Insert the following text at the end of this section: “A contractual agreement between the organization and a supplier defining the performance responsibilities and commitments of the suppliers shall be relied upon to fulfill documentation requirements related to this section.“
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 353	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.10.5.1	Comment
	Reference: “The organization shall review and follow security requirements before undertaking any unplanned maintenance on any component of the AMI system. Unplanned maintenance must be documented and include the following: 1. The date and time of maintenance; 2. The name of the individual(s) performing the maintenance; 3. A description of the maintenance performed; If physical access or modification is required, also document the following: • The name of the escort, if necessary;

Comment Number: 353	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

- A list of equipment removed or replaced (including identification numbers, if applicable)."

Rationale/Recommendation

THIS REQUIREMENT COULD CREATE CONFLICT WITH THE PERFORMANCE OF MAINTENANCE WITHIN THE COMMERCIAL CARRIER NETWORK. THE COMMERCIAL CARRIER MUST RETAIN CONTROL OF ITS OPERATIONAL PROCEDURES.

Revise this section as follows: "The organization shall review and follow security requirements before undertaking any unplanned maintenance on any component of the AMI system under its direct control. Commercial service providers delivering AMI components shall keep records according to their existing procedures or as provided by a contractual agreement with the organization. Unplanned maintenance that is performed by the organization or under its direct control must be documented and include the following:

1. The date and time of maintenance.

2. The name of the individual(s) performing the maintenance.

3. A description of the maintenance performed; If physical access or modification is required, also document the following:

- The name of the escort, if necessary;
- A list of equipment removed or replaced (including identification numbers, if applicable)."

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 354	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4	Comment
	Reference: "The organization schedules, performs, and documents routine preventive and regular maintenance for

Comment Number: 354	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

DHS-2.10.6.1	all components of the AMI system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures.
	Rationale/Recommendation
	Insert the following text at the end of this section: “Commercial service providers shall adhere to their existing maintenance practices or those practices defined in contractual agreements with the organization.
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 355	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.10.9.1	Comment
	Reference: “The organization shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities on all components of the AMI system. When remote maintenance is completed, the organization or AMI component must terminate all sessions and remote connections invoked in the performance of that activity. “
	Rationale/Recommendation
	THESE REQUIREMENTS APPEAR TO BE DIRECTED TO DEVICES THAT ARE UNDER THE DIRECT CONTROL OF UTILITIES. A SERVICE PROIDER SHOULD BE OBLIGATED TO NOTIFY AND WORK WITH UTILITIES WHEN REMOTE MAINTENANCE IS PERFORMED ON AMI COMPONENTS RESIDING ON THE SERVICE PROVIDER’S NETWORK. HOWEVER, SINCE MAINTENANCE ACTIVITIES ARE PERFORMED ON A COMMERCIAL NETWORK SUPPORTING MANY CUSTOMERS, THE SERVICE PROVIDER SHOULD NOT BE REQUIRED TO SEEK PERMISSION FROM UTILITIES BEFORE MAINTENANCE IS PERFORMED. Revise this section as follows: “The organization shall authorize, manage, and monitor remotely executed maintenance and diagnostic activities on all components of the AMI system performed by organization personnel. When remote maintenance is completed, the organization or AMI component must terminate all sessions and remote connections invoked in the performance of that activity. “
	Disposition

Comment Number: 355	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 356	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.12.2.1	Comment	
	Reference: “The organization shall develop and implement a continuity of operations plan dealing with the overall issue of maintaining or re-establishing operation of the AMI system in case of an undesirable interruption. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan. “	
	Rationale/Recommendation	
	CLARIFICATION SHOULD BE CONSIDERED REGARDING THE ROLES AND RESPONSIBILITIES OF THE ORGANIZATION AND AUTHORITY/CONTROL OVER THE BUSINESS CONTINUITY OPERATIONS OF SUPPLIERS. Revise this section as follows: “The organization shall develop and implement a continuity of operations plan dealing with the overall issue of maintaining or re-establishing operation of the AMI system in case of an unanticipated interruption. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan for the organization’s personnel. Commercial service providers participating in the AMI system shall, pursuant to appropriate protection, disclose their business continuity plan (“BCP”) to and work with the organization to assure such plans can meet AMI system requirements.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 357	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.12.4.1	Comment	
	Reference: "The organization shall train personnel in their continuity of operations plan roles and responsibilities with respect to the AMI system. The organization provides refresher training annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan. "	
	Rationale/Recommendation	
	THE ORGANIZATION SHOULD BE RESPONSIBLE FOR ASSURING THAT TRAINING IS COMPREHENSIVE AND UP-TO-DATE. Revise this section as follows: "The organization is responsible for obtaining validation that personnel are trained to fulfill continuity of operations plan roles and responsibilities with respect to the AMI system and that refresher training occurs no less than annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan. Commercial service providers shall certify training requirements are fulfilled for their BCP disclosed pursuant to DHS-2.12.4.1."	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 358	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.12.8.1	Comment	
	Reference: "The organization must track and document AMI system security incidents on an ongoing basis. "	
	Rationale/Recommendation	
	CLARIFICATION SHOULD BE CONSIDERED AS TO WHAT CONSTITUTES AN INCIDENT. PRECISE METHODS FOR COMPLIANCE SHOULD BE DESIGNED BY THE SUPPORTING PARTY. Insert the following text at the end of this section: "The organization shall define information requirements in contractual language with suppliers to the extent information is required from the supplier to permit this obligation to be met by the organization."	

Comment Number: 358	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 359	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.12.9.1	**Comment**	
	Reference: “The organization promptly reports security incident information to the appropriate authorities. “	
	Rationale/Recommendation	
	THE CONCEPT IS APPROPRIATE; HOWEVER, FURTHER PROCESS DEFINITION MAY BE REQUIRED. Insert the following text at the end of this section: “The organization shall define information requirements (timeliness and detail) in contractual language with suppliers to the extent information is required from the supplier so as to permit this obligation to be met by the organization.”	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 360	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4 DHS-2.12.10.1	**Comment**	
	Reference: “The AMI component vendor must support customers or customer facing organizations with advice and assistance in the handling and reporting of security incidents as appropriate. “	
	Rationale/Recommendation	

Comment Number: 360	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

	THE OBLIGATION THAT MUST BE FULFILLED IS UNCLEAR. Insert the following text at the end of this section: “The organization’s requirement that an AMI component vendor provide customers or customer facing organizations with advice and assistance in the handling and reporting of security incidents shall be set forth in contractual language with the affected component vendor.”
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 361	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.14.12.1	Comment
	Reference: “The organization shall handle and retain output from the AMI system in accordance with applicable laws, regulations, standards, and organizational policy, as well as operational requirements of the AMI system.”
	Rationale/Recommendation
	VENDORS/SUPPLIERS ARE SUBJECT TO THEIR OWN RECORD RETENTION REQUIREMENTS. Insert the following text at the end of this section: “Contractual provisions with suppliers shall include sufficient requirement detail to permit suppliers to self-certify compliance.”
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 362	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 362	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.15.5.1

Comment

Reference: “The organization shall manage AMI system authenticators by:

1. Defining initial authenticator content criteria;

2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;

3. Changing default authenticators upon AMI system installation;

4. Changing/refreshing authenticators periodically;

5. All components must be able to support these organizational activities;

6. All permissions associated with authenticators should be maintained at as low a level as possible so that, in case of compromise, an attacker's access would be limited (see DHS-2.15.9 Least Privilege).”

Rationale/Recommendation

THESE REQUIREMENTS/RESPONSIBILITIES SHOULD SPECIFICALLY APPLY AT THE APPLICATION LAYER. COMPONENT (E.G., COMMUNICATIONS) PROVIDER SHOULD RETAIN CONTROL AND MANAGEMENT OF AUTHENTICATORS THAT ARE PROPRIETARY AND SUPPORT INTERNAL NETWORK OPERATIONS.

Revise this section as follows: “The organization shall manage AMI system authenticators at the application layer by:

1. Defining initial authenticator content criteria;

2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;

3. Changing default authenticators upon AMI system installation;

4. Changing/refreshing authenticators periodically;

Comment Number: 362	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

5. All components must be able to support these organizational activities;

6. All permissions associated with authenticators should be maintained at as low a level as possible so that, in case of compromise, an attacker's access would be limited (see DHS-2.15.9 Least Privilege). “

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 363	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.15.6.1

Comment

Reference: “”The organization must supervise and review the activities of users with respect to the enforcement and usage of AMI system access control. AMI components must provide auditing capability specified in section DHS-2.16.”

Rationale/Recommendation

CLARIFICATION SHOULD BE CONSIDERED.

Insert the following text at the end of this section: “Contracts with vendors/suppliers providing AMI component shall include provisions that the vendor/supplier demonstrate sufficient oversight and control to permit the organization to comply with these obligations.”

Disposition

The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 364	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Comment Number: 364	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.15.14.1	Comment
	Reference: “The AMI component/system shall employ authentication methods that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. Must comply with FIPS 140-2 and NERC security authentication method requirements. “
	Rationale/Recommendation
	THIS MAY BE CHALLENGING SINCE SOME AMI COMPONENTS DO NOT COMPLY WITH FIPS 140-2. FOR EXAMPLE, AES IS THE ONLY FIPS COMPLIANT ALGORITHM – HOWEVER, MANY AMI COMPONENTS HAVE PROPRIETARY ALGORITHMS IMPLEMENTED. FURTHERMORE, WHILE THE SERVICE PLATFORM FOR A COMMUNICATIONS SERVICE MIGHT MEET FIPS 140-2, THE UNDERLYING COMPONENTS ARE NOT LIKELY TO HAVE BEEN INDIVIDUALLY CERTIFIED FIPS 140-2 COMPLIANT AND NO PRACTICAL PURPOSE WOULD BE SERVED BY UNTERTAKING SUCH A CERTIFICATION. Revise this section as follows: “The AMI component/system shall employ authentication methods that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. The organization is responsible for assuring compliance with FIPS 140-2 and NERC security authentication method requirements at the component and systems for elements owned by the organization and at the service level for elements obtained from commercial service providers. “
	Disposition
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.

Comment Number: 365	Submitted by: AT&T	Comment Type: _X_ Technical __ Editorial __ General

Reference: Chapter 4 DHS-2.16.3.1	Comment
	Reference: “All AMI components must capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes. “
	Rationale/Recommendation
	SERVICE PROVIDERS SHOULD HAVE PROCEDURES TO CAPTURE DETAILED AUDIT RECORDS AND

<table>
<tr><td colspan="2">Comment Number: 365</td><td>Submitted by: AT&T</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td></td><td colspan="3">OTHER INFORMATION IN THEIR NETWORK.
Insert the following text at the end of this section: “All AMI components under the direct control of the organization must capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes. Commercial service providers delivering AMI components shall document and follow and periodically internally audit compliance with procedures designed to capture equivalent information for communications capabilities supplied as part of the AMI system.”</td></tr>
<tr><td></td><td colspan="3">Disposition</td></tr>
<tr><td></td><td colspan="3">The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 366</td><td>Submitted by: Center Point Energy</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td>Reference: Overall</td><td colspan="3">Comment</td></tr>
<tr><td></td><td colspan="3">The U.S. Department of Homeland Security (DHS) similarly emphasizes the need for balance in its control systems security recommendations,[5] which NIST referenced in creating its Draft Report. As part of its recommendations, DHS states that “[t]he goal of a control systems security program is to balance security while operating within resource limits. . . . Security is not to impede operation. . . . The most successful security program is one that integrates seamlessly and becomes a common aspect of daily operation.”[6] As written, and at least in isolation, the Draft Report does not allow for much balance. That is, there is no rule of reasonableness to be applied by the utility, nor are alternative security measures contemplated that would provide adequate protection. To the contrary, it appears as if the requirements (and the supplemental guidance and enhanced requirements as well) outlined in the Draft Report are to be followed regardless of cost or other contravening measures.</td></tr>
<tr><td></td><td colspan="3">Rationale/Recommendation</td></tr>
</table>

[5] Department of Homeland Security, National Cyber Security Division. 2008, January. Catalogue of Control Systems Security: Recommendations for Standards Developers. Retrieved from http://www.us-cert.gov/control_systems/.

[6] *Id*. at 2 (underline added).

Comment Number: 366	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General

	None
	Disposition
	The second draft of the NISTIR includes a discussion of compensating controls, that cost needs to be considered, and that this is a guidance document – as a starting point for any organization. We will consider this comment as we develop the next version of the NISTIR.

Comment Number: 367	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General

Reference: Overall	Comment
	In order to strike the right balance, it is imperative that any cyber security program be governed by risk-based performance standards, not by security-specific requirements. The Company cannot overstate the need for flexibility in reaching the desired security ends. The DHS recommendations, again, are instructive: “Decisions regarding when, where, and how these standards should be used are best determined by specific industry sectors. This document provides those decision-makers with a common catalogue (framework) from which to select security controls for control systems.”[7] Importantly, not just specific industry sectors but the companies themselves should play a significant role in deciding when, where, and how standards should be used. Give industry a desired end, and let it determine how best to get there. The diversity of solutions offered by risk-based performance standards benefits the goal of increased security for other reasons. For instance, hackers may prove more effective homing in on prescriptive, detailed solutions published in the Draft Report, where they know exactly what they are confronting when attempting to disrupt a utility’s Smart Grid.
	Rationale/Recommendation
	Utilize Risk-Based Performance Standards.
	Disposition
	The second draft of the NISTIR includes a discussion of compensating controls, that cost needs to be considered, and that this is a guidance document – as a starting point for any organization. We will consider this comment as

[7] *Id.* at 1.

Comment Number: 367	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
	we develop the next version of the NISTIR.	

Comment Number: 368	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Overall	Comment	
	Although CEHE understands NIST's role in creating standards (or requirements), the Company is less clear which agency or agencies, and at which level (State or Federal), will have ultimate enforcement authority in this area. Without a named responsible agency, for instance, there can be no assurance that FERC/NERC will be the enforcement authority. Even assuming FERC will have enforcement authority, it is unclear whether another Federal agency, such as DHS, will have a coordinating role in crafting policy and regulations. The Company understands that there are several efforts ongoing at the Federal level to legislate cyber security. In the meantime, however, without knowing the amount of institutional knowledge the eventual enforcement authority will have, CEHE is without sufficient knowledge to best tailor its comments. Consequently, CEHE asks that it and others be given an additional opportunity to comment on any standards, requirements, or regulations after jurisdictional issues at the Federal level related to cyber security are resolved. Further, it appears as if there may be at least two sets of requirements emerging at the Federal level relating to cyber security—i.e. these NIST requirements and NERC-CIP requirements—as well as security requirements that exist at the State level. It is important that utilities such as CEHE be bound by only standards and requirements that are complementary. At the Federal level, the NERC-CIP standards already cover bulk electric transmission, so new requirements related to the Smart Grid should not be inconsistent or redundant. Federal regulations in this area also raise concerns at the State level. For instance, the Draft Report and its use cases apply to a more traditional vertically integrated utility and make no allowances for the deregulated model in Texas. The language relating to Home Area Network ("HAN") devices which would place all security responsibility on the TDU is completely inconsistent with the existing Texas market, where many if not most of the HAN devices will neither be owned nor controlled by the TDU. Employing a regulatory construct governed by risk-based performance standards provides a practical way to overcome these issues. Moreover, although CEHE has no objection to the Federal government having ultimate regulatory authority over cyber security of the Smart Grid—particularly with FERC/NERC as the Federal point of contact—the Company believes that State authorities should have the enforcement authority over the regulations.	
	Rationale/Recommendation	
	Responsibility for Enforcement Authority Should Be Announced.	

Comment Number: 368	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
	Disposition	
	The enforcement authority is outside the scope of the SGIP-CSWG. NIST is discussing this issue with FERC, NERC, NARUC, and the state PUCs.	

Comment Number: 369	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	The Company believes that a few areas concerning audits in the Draft Report need revision and/or clarification. Throughout Section DHS – 2.16, for instance, the term “audit” is used to describe both management monitoring responsibility and independent audit activity. A more detailed definition of “audit” and “independent audit” is required. The same section mentions that audits “can be either in the form of internal self-assessment or independent, third-party audits.” Does this mean companies can choose which audit is performed? Similarly, regarding the language “selection of auditors”: Does this imply that companies will have the ability to select who will audit them? Finally, there is an apparent inconsistency arising from DHS – 2.16.14.1. This requirement seems to state that internal audits can perform reviews. This seems to conflict with DHS-2.16.11.2, which states independent reviews are required for audits beyond documentation reviews. As to Section ASAP-2.16.13.2, which describes the measures that need to be taken to safeguard audit tools, is the Draft Report referring to audit tools used in monitoring activities (e.g., logs, reports, etc.) or tools used to conduct an audit (e.g., ACL, TeamMate, etc.)? Some of the tools that may be used to conduct an audit are available freely on the Internet (e.g., NMAP, Snort, etc.). How are companies supposed to “protect” these Advanced Meter Infrastructure (“AMI”) system audit tools from misuse or compromise?	
	Rationale/Recommendation	
	Audit Provisions Should Be Clarified.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 370	Submitted by: Center Point Energy	Comment Type: _x_ Technical __ Editorial _X_ General
Reference: Appendix A	Comment	
	Appendix A states, in relevant part: "Power system operations must be able to continue during any security attack or compromise (as much as possible)." CEHE concurs with this statement. The Company would emphasize, however, that it is unreasonable to think that all power system operations must continue during any security attack.	
	Rationale/Recommendation	
	This statement should be refined to demonstrate that some portion of a power system can cease operations without an objectionable impact on the overall power system.	
	Disposition	
	Agree. This wording will be addressed in the next version of the NISTIR.	

Comment Number: 371	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Appendix A	Comment	
	There are many locations in Appendix A where the term "critical to distribution operations" is used. This can be a misleading use of the term "critical" and confused with the use of the term "critical" in the NERC-CIP standards. For instance, "critical to the distribution system" is not necessarily "critical" to the Bulk Power System. CEHE therefore advocates the use of a different term.	
	Rationale/Recommendation	
	None	
	Disposition	
	We will evaluate the use of the term "critical" in the next version of the NISTIR. Currently the word is used in context unrelated to NERC-CIP.	

Comment Number: 372	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference:	Comment	

Comment Number: 372	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General

Page D-15	On page D-15 of Appendix D, the last comment states: “There is probably a need for intersection of security at various layers.” The Company believes there is not only a need for security at various layers, but also within networks and—for example, in Texas where the data of different TDUs will be stored in the Smart Meter Texas Common Repository.
	Rationale/Recommendation
	None
	Disposition
	Consensus was not to change this statement because it includes networks.

Comment Number: 373	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 1.3	Comment
	Sec 1.3. The second bullet item on page 3 provides a definition of Cyber Security, and indicates that the definition is for this document.
	Rationale/Recommendation
	The Company believes that this definition is different than the NERC-CIP definition of Cyber Security, and that the definitions should be the same.
	Disposition
	We have revised the definition of cyber security to be more inclusive of the information technology, telecommunications, and electric sectors.

Comment Number: 374	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General

Reference: Section 1.4	Comment
	The Company is not sure what is meant by “requirements . . . will apply to the Smart Grid as a whole” and seeks clarification. It is unclear whether this language implies that each utility segment, including individual meters, should be met with the same amount of security. Such an interpretation would be inconsistent with the Federal government’s security approach—and, indeed, this Draft Report—which is predicated on risk. Various segments of the Smart Grid

Comment Number: 374	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General

clearly have different risk profiles. The most obvious example is the individual meter, which poses much less risk to the Smart Grid than, for instance, a unit in the transmission system. Therefore, each segment within the Smart Grid should be secured based on the amount of risk it poses to the Smart Grid.

Moreover, Section 1.4 of the Draft Report implies that all standards are specified by a risk analysis, which is not necessarily correct. The language does not allow utilities to perform their own risk analysis, yet seems to indicate that this NIST document can prescribe all of the necessary cyber security requirements. It appears as if, by stating that NIST will identify all standards and gaps, there is no need for utilities to complete their own analysis and simply accept the one-size-fits-all approach. CEHE strongly recommends that NIST acknowledge the inherent cyber security value of allowing multiple approaches to meet common performance goals over a one-size fits all approach, and the role that individual utilities should perform in conducting risk analyses and implementing solutions.

Rationale/Recommendation

Propose the following changes to Section 1.4, which states, in relevant part: "The risk assessment process for the Smart Grid will be completed when the security requirements are specified. These requirements will be selected on the basis of a risk assessment and will apply to the Smart Grid as a whole. The requirements will not be allocated to specific systems, components, or functions of the Smart Grid. In specifying the security requirements, to the extent practical gaps will be identified. The implementation, assessment and monitoring of security controls are applicable when a system is implemented in an operational environment. The output from the Smart Grid risk management process should be used in these steps. In addition, if feasible, the full risk management process should be applied to legacy systems and when Smart Grid owners and operators implement new systems or augment/modify existing systems."

Disposition

In the second draft of the NISTIR we have revised the wording to address this comment.

Comment Number: 375	Submitted by: Center Point Energy	Comment Type: __ Technical __ Editorial _X_ General

Reference: Section 2.1

Comment

Section 2.1. Any attempt to define Personally Identifiable Information (PII) must account for rules and definitions of PII in other jurisdictions. This document appears to be creating PII within this section. This section arguably is inappropriate and should merely suggest that utilities follow State guidelines on privacy. Where States have not

Comment Number: 375	Submitted by: Center Point Energy	Comment Type: __ Technical __ Editorial _X_ General

defined privacy, it is incumbent upon utilities to provide definitions within their respective organizations and to work with state regulators to develop appropriate rules. There is also a difference between data privacy and data security. NIST should focus on data security issues, and especially upon data security that effectively frustrates security breaches that result in identity theft.

Rationale/Recommendation

None

Disposition

In the second draft of the NISTIR we have revised the content of the privacy section. The revised content does not use the term PII.

Comment Number: 376	Submitted by: Center Point Energy	Comment Type: __x Technical __ Editorial __ General

Reference: Section 2.4

Comment

Section 2.4. “"Areas of the electric system that cover the scope of a Smart Grid include the following:

> the delivery infrastructure (e.g., transmission and distribution lines, transformers, switches),… management of the generation and delivery infrastructure at the various levels of system coordination (e.g., transmission and distribution control centers, regional reliability coordination centers, national emergency response centers),”

In general, the transmission systems are already automated and operate as “smart systems.” If some entities contemplate further automation of their transmission infrastructure to support the deployment of a Smart Grid, existing standards should be utilized, not contradicted or inadvertently amended by these standards or any other new standards under development. If standards referring to transmission systems need to be revised to better support Smart Grid deployment in the distribution area, then the existing standards should be modified to include the necessary revisions. At the outset, it is critically important to recognize that cyber-security concerns at the transmission level differ significantly from those applicable to distribution systems.

Rationale/Recommendation

The scope of Smart Grid should be limited to the automation of the distribution systems between the transmission system and the end use customer.

Disposition

<table>
<tr><td colspan="2">Comment Number: 376</td><td>Submitted by: Center Point Energy</td><td>Comment Type: __x Technical __ Editorial __ General</td></tr>
<tr><td></td><td colspan="3">In the second draft of the NISTIR the privacy section has been revised and this text was removed..</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 377</td><td>Submitted by: Center Point Energy</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="6">Reference: Section 2.5</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">In Texas, individual usage data collected by smart meters is generally considered to be confidential and is owned by the customer. TEX. UTIL. CODE ANN. §§ 32.101(c) and 39.107(b) (Vernon 2009). In implementing these statutes, the Public Utility Commission of Texas (“PUCT”) has specifically identified “proprietary customer information” as meriting special protection. Pub. Util. Comm’n Subst. R. 25.272(c)(5) and 25.472(b)(1). Thus, the PUCT recognizes that there will be different security requirements for the use of operational data that is not PII.</td></tr>
<tr><td colspan="3">Rationale/Recommendation</td></tr>
<tr><td colspan="3">None</td></tr>
<tr><td colspan="3">Disposition</td></tr>
<tr><td colspan="3">Please review the second draft of the NISTIR and submit a comment if this has not been addressed. We are unclear about your recommendation.</td></tr>
</table>

<table>
<tr><td colspan="2">Comment Number: 378</td><td>Submitted by: Center Point Energy</td><td>Comment Type: _X_ Technical __ Editorial __ General</td></tr>
<tr><td rowspan="2">Reference: Section 2.5.3</td><td colspan="3">Comment</td></tr>
<tr><td colspan="3">It should be understood that advanced meters will collect the same customer usage data (registered in 15 minute increments), regardless of the type of retail electric service for which a consumer has contracted. As noted above, however, individual customer data is owned by the customer and cannot be distributed without prior customer consent. There are important exceptions to this principle. In Texas, there are generally four main entities that will receive the data: the TDU, the REP, the PUCT, and ERCOT. Sharing data with each of these entities is a precondition to receiving utility service because each entity performs essential “utility services.” For example, TDUs meter retail consumers’ electric usage and bill the various REPs serving individual consumers for T&D services and provide the detailed usage data to such REPs so that they can also bill the retail consumers for the electric services provided by each REP. The Electric Reliability Council of Texas has individual customer data as the independent system operator, but must keep such data confidential. Finally, the PUCT, of course, has the right to access such data as the governmental authority charged with regulation of electric utility service.</td></tr>
</table>

Comment Number: 378	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
	Rationale/Recommendation	
	NIST should not alter the current carefully balanced structure of the Texas retail electric market concerning access to individual customer usage data, which might be inferred from the discussion in Section 2.5.3. Texas maintains a carefully structured set of laws and regulations concerning the protection of such data. The Company is concerned that certain requirements proposed in the Draft Report may frustrate the balance of this structure, which has proven to be very effective.	
	Disposition	
	The second draft of the NISTIR has been revised to clarify that the information is guidance, not mandatory.	

Comment Number: 379	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Section 2.5.6	Comment	
	Currently, customer information that is held confidential and is owned by the customer, like kWH usage data, is stored for specific purposes, like billing, and will be made available to the consumer upon request. The consumer is not, however, given access to the data in every system in which it is stored. Granting such access would create an unnecessary and unreasonable security risk, since the data is stored in secure systems within the utility.	
	Rationale/Recommendation	
	None	
	Disposition	
	Please review the second draft of the NISTIR and submit a comment if this has not been addressed. We are unclear about your recommendation.	

Comment Number: 380	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	The NIST requirements below fall into the category of currently evolving technology. After reviewing the requirements below, CEHE understands that they will be met in its system over the next two to five years. The components that make up the AMI system are not mature, and the vendors who manufacture this equipment are	

Comment Number: 380	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
	continuously working to include new security enhancements in future releases of their products. In many of the requirements listed below, the document states that meeting the requirement is “problematic” in an AMI component. In these cases, products must become commercially available and technological solutions must be developed before the requirement should be enforceable. DHS 2.8.3 Security function Isolation (specifically DHS 2.8.3.1), DHS 2.8.5 Denial of Service Protection (specifically DHS 2.8.5.1, DHS 2.8.5.2), DHS Boundary Protection (specifically DHS 2.8.7.1, DHS 2.8.7.2), DHS 2.8.11 Cryptographic Key Establishment and Management, DHS 2.8.14 Transmission of Security Parameters (specifically DHS 2.8.14.1), DHS 2.10.9 Remote Maintenance (specifically DHS 2.10.9.1), DHS 2.12.8 Incident Monitoring (specifically DHS 2.12.8.3), DHS 2.14.4 Malicious Code Protection (All), DHS 2.14.7 Software and Information Integrity (specifically DHS 2.14.7.1), DHS 2.14.10 Information Input Accuracy, Completeness, Validity, and Authenticity (All), DHS 2.14.11 Error Handling (All), DHS 2.15.18 Concurrent Session Control (All), DHS 2.15.20 Unsuccessful Login Attempts (All), DHS 2.15.21 Session Lock (All), DHS 2.15.22 Remote Session Termination (All), DHS 2.15.30 Unauthorized Reporting (All), DHS 2.16.2 Auditable Events (specifically DHS 2.16.2.1), DHS 2.16.3 Content of Audit Records (specifically DHS 2.16.3.1), DHS 2.16.4 Audit Storage Capacity (All), DHS 2.16.8 Time Stamps (All).	
	Rationale/Recommendation	
	The NIST requirements should be refined to remove statements requiring “all components” to include security features. Many security requirements can effectively be handled in a central “system” method.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 381	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	Requirements where technology exists yet CEHE is using alternate methods to address - The requirements for SPAM Protection (DHS 2.14.8 All), and Access Control (DHS 2.15 All), need to be flexible enough to allow for enterprise class systems. Alternative effective methods of providing these controls should be allowed to meet the requirement. All AMI systems do not require segregation from IT enterprise system management. Enterprise email	

Comment Number: 381	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
	gateway "SPAM" protection and enterprise identity management systems are more effective than distributed solutions. Furthermore, distributed solutions require installation on endpoint components, version and configuration control, and constant monitoring.	
	Rationale/Recommendation	
	In general, the requirements need to be more flexible to allow alternatives that meet the security requirement for efficiency and effectiveness.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 382	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	Requirements where no current technology exists to satisfy - Technology to meet the requirements for Malicious Code Protection as described in DHS 2.14.3.1, DHS 2.14.3.3 does not exist in current meter and HAN end point devices. Furthermore, adding such functionality to these devices could drive the cost of the devices out of the consumer price range and hinder consumer adoption of the technology. NIST states that "field deployed host devices are typically not suitable for traditional third party host based malicious code protection mechanisms."	
	Rationale/Recommendation	
	The requirements in this area need to be flexible enough to allow for reasonable malicious code protections at central points within the AMI system and not on every component.	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	

Comment Number: 383	Submitted by: Center Point Energy	Comment Type: _X_ Technical __ Editorial __ General
Reference: Chapter 4	Comment	
	Requirements that are not clear and need further detail - The requirements listed below need further clarification for AMI implementers to be able to evaluate the impact to the current and planned implementation. It is not clear what is being recommended here and what the requirements will be. DHS 2.8.17 Voice Over Internet Protocol (All), DHS 2.8.20 Message Authenticity (All), DHS 2.8.21 Architecture for Provisioning Name/Address Resolution (All), DHS 2.8.22 Secure Name/Address Resolution Service (All), DHS 2.12.18 Fail-Safe Response (All).	
	Rationale/Recommendation	
	None	
	Disposition	
	The second draft of the NISTIR includes requirements for the entire Smart Grid. The AMI requirements included in the first draft of the NISTIR were developed by the ASAP-SG project as part of the AMI Security Profile document which is now being maintained by the UCAIug SG Security working group. This comment has been forwarded to SG Security WG for disposition.	